město Bystřice nad Pernštejnem
Příční 405, 593 01 Bystřice nad Pernštejnem
tel.: 566 590 311, e-mail: posta@bystricenp.cz, ID datové schránky: b3mbs36

SMĚRNICE

vztahující se k Nařízení Evropského parlamentu a Rady (EU) 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), dále v textu směrnice jen jako *„GDPR“* nebo *„Nařízení“*

o zpracování a volném pohybu osobních údajů fyzických osob vydaná dne 25.05.2018 u správce, kterým je

město Bystřice nad Pernštejnem,
Příční 405, IČ: 002 94 136,
593 01 Bystřice nad Pernštejnem
(dále v textu směrnice jen jako „Město“ nebo „Správce“)

Článek I.
Úvodní ustanovení - vymezení působnosti směrnice

Směrnice je aplikací ochrany údajů fyzických osob a jejich soukromí v souvislosti s jejich zpracováním a o volném pohybu těchto údajů v organizacích (obcích) tak, aby bylo dosaženo požadované ochrany údajů fyzických osob, jejichž údaje organizace (obec) zpracovává v rámci svojí činnosti.
Směrnice je aplikací 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 (General Data Protection Regulation - GDPR) a vstupuje v platnost 25. května 2018.
Jejím cílem je přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektu údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu Obecného nařízení a dozoru jednotlivými dozorovými úřady.
Směrnice upravuje postupy zaměstnanců Města/Správce při zpracování osobních údajů, zejména při jejich získávání, shromažďování, ukládání, použití, šíření a uchovávání.
Směrnice je závazná nejen pro zaměstnance Města, kteří v rámci své činnosti zpracovávají osobní údaje fyzických osob, ale i pro zaměstnance, kteří v rámci plnění svých pracovních povinností nepřicházejí do běžného styku a touto agendou.

Článek II.
Vymezení/definice pojmů v souladu s GDPR (článek 4) Nařízení

Zaměstnanci se při výkonu svých pracovních povinností mohou setkat s těmito pojmy, které jsou blíže definovány Nařízením:

„**Osobními údaji**“ se rozumí veškeré informace o identifikované nebo fyzické identifikovatelné osobě (dále jen „subjekt údajů“); typicky jde o jméno, příjmení a adresu, datum narození, rodné číslo, státní občanství, telefonní číslo atp.; Osobním údajem je rovněž každá informace o fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

„**Zvláštním (citlivým) osobním údajem**“ je takový údaj, který vypovídá o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu, či o sexuálním životě, nebo sexuální orientaci fyzické osoby, genetické a biometrické údaje. Se zpracováním těchto údajů musí subjekt udělit výslovný souhlas.

„**Zpracováním**“ se rozumí 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; Jakékoliv osobní údaje jsou městem zpracovávány zákonným způsobem na základě zákona, nebo se souhlasem subjektu, jehož údaje se zpracovávají.

„**Omezením zpracování**“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

„**Profilováním**“ 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;

„**Pseudonymizací**“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

„**Evidencí**“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

„**Správcem**“ je Město, které samo nebo společně s jinými správci určuje účely a prostředky zpracování osobních údajů;

„**Zpracovatelem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro Správce;

„**Příjemcem**“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterému jsou osobní údaje poskytnuty. Orgány veřejné moci, které mohou získávat osobní údaje v rámci výkonu svých vyšetřovacích pravomocí, se za příjemce nepovažují;

„**Třetí stranou**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, Správcem, zpracovatelem ani osobou přímo podléhající Správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;

„**Souhlasem**“ 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;

„**Porušením zabezpečení osobních údajů**“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

„**Dozorovým úřadem**“ nezávislý orgán veřejné moci zřízený členským státem podle článku 51; 4.5.2016 L 119/34 Úřední věstník Evropské unie CS;

Článek III.
Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů:

a) poskytuje Městu a jeho zaměstnancům, kteří provádějí zpracování osobních údajů, informace a poradenství o jejich povinnostech vyplývajících z GDPR a dalších příslušných právních předpisů v oblasti ochrany osobních údajů;

b) monitoruje soulad činností Města a jeho zaměstnanců s GDPR a dalšími příslušnými právními předpisy v oblasti ochrany osobních údajů;

c) zvyšuje odborné povědomí a přípravu zaměstnanců, kteří zpracovávají osobní údaje a provádí související audity;

d) poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitoruje jeho uplatňování;

e) spolupracuje s dozorovým úřadem a působí pro něj jako kontaktní místo.

Článek IV.
Sídlo/popis sídla Správce a jeho odborů; zabezpečení Správce

Správce má sídlo v pětipodlažní budově která je v majetku města.

V prvním nadzemním podlaží sídlí vedení města, Odbor správní a školství. Ve druhém nadzemním podlaží sídlí Odbor financí a obecního živnostenského úřadu a Odbor správy majetku a investic. Ve třetím nadzemním podlaží sídlí Odbor správní a školství – oddělení správní, odbor správní a školství – oddělení školství a odbor sociálních věcí a zdravotnictví. Ve čtvrtém nadzemním podlaží sídlí Odbor dopravy a silničního hospodářství a Odbor životního prostředí. V pátém nadzemním podlaží sídlí Odbor územního plánování a stavebního řádu a odbor bytového hospodářství.

Archiv je umístěn v prvním podzemním podlaží. Celý objekt je zabezpečen zabezpečovacím zařízením s pohybovými čidly. V případě neoprávněného vniknutí systém upozorní osoby nebo externí správce určené Správcem.

Článek V.
Povinnosti zaměstnance vyplývající z GDPR
Povinnosti Správce a zpracovatelů vyplývající z GDPR – OBECNĚ
(některé povinnosti/situace/postupy jsou rozpracovány dále v směrnici/příslušných směrnicích/řádech nebo pokynech tajemníka)

Zaměstnanec je povinen:

a) **zachovávat mlčenlivost** o skutečnostech, o kterých se dověděl při výkonu své pracovní činnosti;
b) **zpracovávat osobní údaje subjektu údajů jen na základě pokynů zaměstnavatele**, které jsou udělovány buďto prostřednictvím zaměstnavatele samotného nebo prostřednictvím vedoucích zaměstnanců;
c) dbát na korektní a přesné zpracování osobních údajů;
d) **neprodleně informovat** zaměstnavatele nebo vedoucího zaměstnance v případě, když, podle jeho názoru, dojde k porušení rámce zpracování osobních údajů;
e) **ohlásit zaměstnavateli jakékoliv porušení zabezpečení Osobních údajů** nebo podezření na porušení zabezpečení Osobních údajů, a to nejpozději v den zjištění takového porušení nebo takového podezření. Toto učiní buďto přímo zaměstnavateli nebo vedoucímu zaměstnanci nebo firemnímu IT specialistovi s tím, že toto hlášení bude vždy podpořeno mailovou zprávou nebo zápisem ohlášení podepsaným oběma účastníky ohlášení. Pracovník, kterému byl incident nahlášen, postupuje dál v souladu s touto směrnicí, a to podle stupně závažnosti hlášeného incidentu (článek Porušení zabezpečení osobních údajů);
f) **ohlásit jakoukoliv náhodnou/nahodilou manipulaci s Osobními údaji**, kterou došlo k vymazání dat subjektů údajů. Ohlášení pro případy definované e) a f) bude obsahovat popis povahy daného případu a množství subjektů dotčených atakem třetí osoby nebo nechtěným vymazáním/popř. neoprávněným přenosem dat subjektu údajů/subjektů údajů;
g) **skartovat listiny**, které jsou určené ke skartaci přímo na pracovišti nebo v nejbližší místnosti ke skartaci určené;
h) zachovávat na svém pracovišti takový stupeň pořádku, aby ze zanechaných listin (poznámek, pomocných tisků ze systému, konzultačních listů…) na pracovním místě nehrozil únik osobních údajů subjektu údajů. Je **povinen zachovávat zásadu tzv. „čistého stolu“**, tj. na pracovním stole nesmí zůstat žádné dokumenty/listinná spisová materie obsahující osobní údaje;
i) **zachovávat zásadu tzv. „čisté obrazovky“**, tj. na ploše/obrazovce počítače nesmí uchovávat žádné dokumenty s osobními údaji, u kterých by hrozilo zneužití dokumentů a dat na nich náhledem a případným přímým atakem třetí osoby. Tato zásada platí pro případ, kdy je Zaměstnanci Zaměstnavatelem svěřen do užívání osobní přenosný počítač pro možnou občasnou práci „mimo úřad“;
j) **chránit elektronický „čip“**, který mu byl Zaměstnavatelem svěřen pro vstup do budovy před ztrátou/poškozením/odcizením nebo zničením. Zaměstnanec je povinen v případě ztráty/poškození/odcizení nebo zničení tohoto „čipu“ nahlásit neprodleně (do 24 hod) jeho ztrátu/poškození/odcizení/zničení na sekretariát Správce nebo vedoucímu zaměstnanci nebo pověřenému IT specialistovi. O tomto úkonu bude sepsán jednoduchý zápis;
k) **chránit bezpečnostní klíč**, který mu byl Zaměstnavatelem svěřen pro vstup do budovy před ztrátou/poškozením/odcizením nebo zničením. Zaměstnanec je povinen v případě ztráty/poškození/odcizení nebo zničení tohoto klíče nahlásit neprodleně (do 24 hod) jeho ztrátu/poškození/odcizení/zničení na sekretariát Správce nebo vedoucímu zaměstnanci nebo tajemníkovi Správce. O tomto úkonu bude sepsán jednoduchý zápis;

l) **neposkytovat v telefonickém kontaktu osobní údaje ze spisové agendy, které podléhají ochraně dle GDPR**. Údaje budou poskytovány pouze a jen na základě dotazů doručených Správci prostřednictvím datových schránek nebo mailů s elektronicky zaručeným podpisem a pouze a jen subjektům oprávněným k příjmu a zpracování osobních údajů;
m) **dbát na ochranu dat** v tom smyslu, že nesmí kopírovat spisovou materii obsahující citlivé údaje subjektů dat na paměťové nosiče datových informací;
n) pro případ, že pracuje s **občanskými průkazy nebo jinými doklady prokazujícími totožnost** subjektu údajů, aby vždy důsledně vykomunikoval souhlas s pořízením fotokopie dokladu (OP nebo cestovní pas) se subjektem údajů, který následně souhlas potvrdí svým podpisem.

Dále pak obecně:

o) Správce a zpracovatelé z jednotlivých odborů **přijímají údaje v rámci své činnosti v písemné i elektronické podobě**. V elektronické podobě přes datovou schránku, email, nebo webové rozhraní. Podle určení údaje a druhu, je ukládají na místo stanovené podle obsahu obdrženého údaje v písemné podobě nebo je zpracovává a ukládá na určené místo v elektronické podobě.
p) Správce a zpracovatelé z jednotlivých odborů **zpracovávají pouze zákonem určené údaje** subjektů údajů, nezbytných pro jeho činnost a s tím souvisejících agend.
q) Správce a zpracovatelé jednotlivých údajů si pro výkon svojí činnosti mohou vést **pomocnou dokumentaci a evidenci**, která obsahuje osobní údaje fyzických osob. Pomocná dokumentace je vedena k zákonnému zpracování údajů v rámci činnosti Správce. U některých pomocných dokumentů je pro jejich zpracování nutný souhlas subjektů údajů.
r) písemná data obsahující osobní údaje fyzických osob jsou mimo pracovní dobu **uložena v uzamykatelných skříních a skříňkách** v sídle Správce.
s) **aktuálně nepoužívaná písemná dat jsou uložena v archivu** Správce.
t) **elektronická data jsou uložena v úložištích dat** – osobních počítačích Správce a zpracovatelů. Z důvodu zabezpečení dat jsou počítače Správce, zpracovatelů a uživatelů při spuštění logována jménem a heslem. Správce, nebo jím pověřený zpracovatel, vlastní pro přístup do aplikací, které využívají v souvislosti se svojí činností certifikát.
u) **úložiště dat jsou v zabezpečených místnostech**, uzamčených skříních nebo skříňkách v sídle Správce. Ukládaná elektronická data jsou zálohována včetně software, který je zpracovává. Počítače mají síťovou ochranu a baterie, které při vypnutí dodávky energie zajistí bezpečné uložení rozpracovaných dat.
v) všechna elektronická **úložiště jsou opatřena aktuálními antivirovými programy**.
w) Správce má na jím určeném místě **centrální úložiště klíčů**, kde má uloženy klíče od písemných a elektronických úložišť dat. Zároveň vede interní knihu výdeje klíčů.
x) všechny osobní počítače, tablety, notebooky a úložiště dat, které jsou majetkem Správce, musí být **zaevidovány**, označeny očíslovány a písemně přiděleny zpracovatelům
y) **doklady s osobními údaji zaměstnanců** (pracovní smlouvy, dotazníky, mzdové listy atd.) v listinné podobě jsou uloženy v kanceláři Správce nebo jím určeného zpracovatele, po dobu pracovního poměru zaměstnance, přičemž Správce může mít tyto údaje i v elektronické podobě. Po skončení pracovního poměru se archivují po dobu 30 let.
z) pracovní smlouvy zaměstnanců musí obsahovat osobní **údaje bezprostředně nutné pro plnění zákonem daných povinností** a zvláštních práv v oblasti pracovního práva, práva v oblasti sociálního zabezpečení, zdravotního pojištění, pro ochranu životně důležitých zájmů subjektu údajů.
aa) **pracovní smlouvy zaměstnanců jsou elektronické i písemné podobě**. Stejně tak vstupní dotazník. Pracovní smlouva zaměstnance obsahuje doložku o souhlasu danému Správci, ke zpracování osobních údajů. Správce nebo zpracovatel zodpovídá za jejich bezpečné uložení proti zneužití Správci.
bb) **Správce používá pro svoji činnost emailovou doménu**. Pro užívání domény má Správce a zpracovatelé svůj email. K tomuto má Správce uzavřenou smlouvu o podmínkách provozu

domény a jejím zabezpečením s jejím Správcem. Smlouva je uzavřena dle směrnice EU 2016/679 a předkládá jí zpracovateli Správce domény.

cc) **Správce v souvislosti se svojí činností může využívat externí zpracovatele**. Správce musí mít v tomto případě uzavřenou smlouvu, kde jsou přesně stanoveny podmínky spolupráce, zejména v případech, kdy externí zpracovatel při svojí činnosti pracuje se subjekty údajů Správce. Zpracovatel odpovídá Správci za bezpečné uložení dat, které mu poskytuje Správce k zajištění jeho činnosti. Správce je oprávněn kontrolovat a dohlížet na uložení jeho dat u zpracovatele. Zpracovatel zpracovává údaje subjektů údajů v souladu s platnými zákony a jeho novelizacemi a aktualizacemi a za správné ukládání a práci s doklady obsahující údaje subjektu údajů odpovídá Správci. Správce má se zpracovatelem uzavřenou smlouvu obsahující podmínky GDPR.

dd) Správci a zpracovatelé **nesmí v přidělených služebních vozidlech**, nebo svých soukromých vozidlech, která využívají v rámci své činnosti ke služebním účelům, **zanechat bez dozoru písemné a elektronické materiály zejména pak s osobními údaji fyzických osob** související s jejich činností. Po opuštění vozidla nesmí bez dozoru zanechat ve vozidle přidělený služební notebook, tablet či mobilní telefon. Veškeré zcizení nebo zneužití osobních údajů fyzických osob je Správce i zpracovatel povinen nahlásit pověřenci.

ee) **všichni zpracovatelé u Správce jsou poučeni a proškoleni o práci s osobními údaji v rámci své činnosti**. Odpovídají Správci za řádné logování osobních počítačů (notebooků) a nutnost chránit osobní údaje fyzických osob zjištěných a převzatých v rámci své činnosti pro správce. Správce vede záznam o jejich proškolení.

ff) Správce pro svou činnost může mít zřízené **webové stránky**. Zde může zveřejňovat údaje v souladu s Nařízením Evropské unie a Rady 2016/679.

gg) **Správce může pořizovat audio, video nahrávky a fotografie subjektů údajů a dále s nimi pracovat v souladu s Nařízením Evropské unie a Rady 2016/679**.

Článek VI.
Bezpečnostní opatření k zajištění ochrany osobních údajů - incidenty

Minimální technická opatření k zajištění ochrany osobních údajů

1) Zaměstnanec, který zpracovává osobní údaje, je povinen:

   a) uchovávat písemnosti a jiné hmotné nosiče osobních údajů pouze v samostatných uzamčených místnostech, případně pouze v □zamč□ný□h skříní□h;

   b) uchovávat elektronické datové soubory obsahující osobní údaje pouze tehdy, je-li přístup k takovýmto souborům nebo přístup k užívání počítače, v jehož paměti jsou tyto soubory umístěny, dostatečně zab□zp□č□ny h□sl□m, či obdobným om□z□ním příst□p□;

   c) zachovávat mlčenlivost o osobních údajích a bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

Minimální organizační opatření k zajištění ochrany osobních údajů

2) Město či jím pověřený zaměstnanec je povinen zajistit:

   a) poučení a seznámení zaměstnanců, kteří zpracovávají osobní údaje, o povinnosti zachovávat mlčenlivost o osobních údajích a bezpečnostních opatřeních, jejichž zveřejnění by oh□ozilo zab□zp□č□ní osobní□h údajů, a to fo□mo□ p□avid□lný□h škol□ní;

   b) pravidelnou kontrolu dodržování povinností vyplývajících z GDPR a dalších příslušných právních předpisů v oblasti ochrany osobních údajů.

Porušení zabezpečení osobních údajů

1) Město či jím pověřený zaměstnanec je odpovědný za evidenci, vyšetření a zdokumentování porušení zabezpečení osobních údajů (dále jen „incidentů“).

2) Město nebo jím pověřený zaměstnanec vede evidenci incidentů, která obsahuje zejména:

   a) □vid□nční označ□ní in□id□nt□;

   b) dat□m a čas odhal□ní in□id□nt□;

   c) □v□d□ní osoby, kt□□á in□id□nt ohlásila;

   d) pod□obný popis in□id□nt□;

   e) dat□m a čas info□mování pověř□n□□ p□o o□h□an□ osobní□h údajů;

   f) vyhodno□□ní in□id□nt□;

   g) datum a čas nahlášení incidentu dozorovému úřadu, byl-li in□id□nt hláš□n;

   h) datum a čas nahlášení incidentu dotčenému subjektu údajů, byl-li in□id□nt hláš□n;

   i) způsob vyřešení incidentu.

3) Při odhalení incidentu je každý zaměstnanec, který incident odhalí, povinen neprodleně písemně informovat Město nebo pověřeného zaměstnance spolu s co nejbližším popisem dotyčného incidentu.

4) Město nebo jím pověřený zaměstnanec zaeviduje incident do evidence incidentů a informuje o něm pověřence pro ochranu osobních údajů.

A) Vyhodnocení incidentu

5) Město nebo jím pověřený zaměstnanec spolu s pověřencem pro ochranu osobních údajů a zaměstnancem, který incident odhalil, nejpozději do 70 hodin od odhalení incidentu provedou vyhodnocení incidentu.

6) V rámci vyhodnocení incidentu se zaznamenají zejména:

   a) příčiny in□id□nt□;

   b) typ in□id□nt□;

   c) určení rizika pro práva a svobody dotčených subjektů údajů v oblasti ochrany osobních údajů;

   d) p□avděpodobné důsl□dky in□id□nt□;

   e) plán nápravných a preventivních opatření.

Typ incidentu

7) Při určení typu incidentu se vychází ze:

   a) skutečnosti, že došlo k neoprávněnému nebo náhodnému poskytnutí nebo zpřístupnění osobních údajů (**porušení důvěrnosti**);

   b) skutečnosti, že došlo k náhodné nebo neoprávněné ztrátě přístupu nebo zničení osobních údajů (**porušení dostupnosti**);

   c) skutečnosti, že došlo k neoprávněnému nebo náhodnému pozměnění osobních údajů (**porušení integrity**).

Rizika incidentu pro práva a svobody dotčených subjektů údajů v oblasti ochrany osobních údajů

8) Při určení rizika incidentu pro práva a svobody dotčených subjektů údajů v oblasti ochrany osobních údajů se vychází z:

   a) typu incidentu;

   b) povahy citlivosti a objemu osobních údajů;

   c) počtu dotčených subjektů údajů;

   d) míry možnosti identifikace jednotlivých subjektů údajů;

   e) závažnost důsledků pro jednotlivé subjekty údajů;

   f) zvláštní charakteristiky jednotlivých subjektů údajů.

9) Při určení rizika pro práva a svobody dotčených subjektů údajů v oblasti ochrany osobních údajů je také nutno zohlednit individuální skutkové okolnosti daného případu.

Výsledek vyhodnocení incidentu

10) Výsledkem vyhodnocení incidentu je prohlášení incidentu za:

   a) nezávažný incident;

   b) středně závažný incident;

   c) vysoce závažný incident.

B) Ohlášení incidentu

Ohlášení nezávažného incidentu

11) Nezávažný incident se nenahlašuje dozorovému úřadu ani dotčenému subjektu údajů. Incident se pouze vyhodnotí.

Ohlášení středně závažného incidentu

12) Středně závažný incident Správce, jím pověřený zaměstnanec nebo pověřenec pro ochranu osobních údajů ohlásí dozorovému úřadu, a to nejpozději do 72 hodin od okamžiku, kdy byl incident odhalen.

13) V ohlášení musí být uvedeno zejména:

   a) jméno a kontaktní údaje Správce a pověřence pro ochranu osobních údajů;

   b) povaha incidentu včetně kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených osobních údajů;

   c) popis pravděpodobných důsledků incidentu;

   d) popis opatření, která Správce přijal nebo navrhl k přijetí s cílem vyřešit daný incident, včetně případných opatření ke zmírnění možných důsledků incidentu.

Ohlášení vysoce závažného incidentu

14) Vysoce závažný incident Správce, jím pověřený zaměstnanec nebo pověřenec pro ochranu osobních údajů ohlásí dozorovému úřadu, a to nejpozději do 72 hodin od okamžiku, kdy byl incident odhalen. Obsah ohlášení je totožný s obsahem ohlášení středně závažného incidentu.

15) Správce, jím pověřený zaměstnanec nebo pověřenec pro ochranu osobních údajů oznámí vysoce závažný incident dotčeným subjektům údajů, a to bez zbytečného odkladu. V oznámení musí být za použití jasných a jednoduchých jazykových prostředků uvedeno zejména:

    a) jméno a kontaktní údaje Správce a pověřence pro ochranu osobních údajů;

    b) povaha incidentu;

    c) popis pravděpodobných důsledků incidentu;

    d) popis opatření, která Správce přijal nebo navrhl k přijetí s cílem vyřešit daný incident, včetně případných opatření ke zmírnění možných důsledků incidentu.

16) Oznámení dotčeným subjektům údajů se nevyžaduje, pokud:

    a) Správce zavedl náležitá technická a organizační opatření, která byla použita u osobních údajů dotčených incidentem, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn mít k nim přístup; nebo

    b) Správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů v oblasti ochrany osobních údajů se již pravděpodobně neprojeví.

17) Pokud by oznámení incidentu subjektům údajů vyžadovalo nepřiměřené úsilí, je Správce, jím pověřený zaměstnanec nebo pověřenec pro ochranu osobních údajů povinen subjekty údajů informovat stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Zabezpečení v oblasti „IT“

1) Do serverovny úřadu mají přístup pouze vybrané osoby pověřené Zaměstnavatelem. Jiným osobám (a to i z řad zaměstnanců nebo vedoucích zaměstnanců) je vstup zakázán.
2) Správce používá vyspělý stupeň antivirové ochrany.
3) Přístup do počítače jednotlivých zaměstnanců je chráněn hesly, u kterých je v časových intervalech prováděno pravidelné obnovování/měnění použitého hesla.
4) Správce provádí pravidelné kontroly připojovaných zařízení, aby nedošlo k ohrožení dat na serveru.
5) Správce používá IT servis odborných IT firem.

Zabezpečení v oblasti personálních záležitostí

1) Pracovníci personálního a účetního oddělení jsou zavázáni k mlčenlivosti o osobních a citlivých údajích zaměstnanců.
2) Pokud není jasně definováno, zda některý údaj je nebo není osobní/citlivý, má se za to, že podléhá mlčenlivosti.
3) Správce má přesně definovaný okruh pravidelně proškolovaných osob, které mají k personálním údajům přístup. V případě nepřítomnosti je zajištěna jejich zastupitelnost.
4) Životopisy (CV) získané při náboru nových zaměstnanců jsou Městem zpracovány následovně – u zájemců, kteří nastoupí do pracovního poměru, se CV stávají součástí zaměstnanecké složky. V této jsou po celou dobu trvání pracovního poměru. PO jeho ukončení jsou skartovány proškoleným pracovníkem personálního oddělení. U nepřijatých uchazečů jsou CV skartována bezprostředně po ukončení výběrového řízení.
5) Personalisté Správce neshromažďují o zaměstnancích Města informace/osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, o zdravotním stavu, sexuálním životě a sexuální orientaci.

Článek VII.
Závěrečná část

1) Správce a Správcem pověření zpracovatelé osobních údajů fyzických osob a osoby s přístupem k osobním údajům fyzických osob v rámci svých pracovních povinností uzavřených na základě pracovní smlouvy se Správcem, jsou povinni tyto osobní údaje fyzických osob chránit proti zneužití před nepovolanými osobami. Jejich zneužití, ztrátu nebo zcizení bezprostředně hlásit pověřenci. Zachovávat mlčenlivost o důvěrných informacích vztahujících se k osobním údajům fyzických osob, o kterých se v této souvislosti dozví.
2) Správce dbá zásadním způsobem na to, aby údaje subjektů údajů, byly vymazány a nebyly dále zpracovávány, pokud již nejsou potřebné pro účely, pro které byly zpracovávány, případně pokud subjekt údajů odvolal svůj souhlas (netýká se zákonného zpracování) se zpracováním a neexistuje žádný další důvod pro zpracování, subjektu údajů vznesl námitku proti zpracování osobních údajů, které se ho týkají, nebo pokud je zpracování jeho osobních údajů v rozporu s nařízením.
3) V případě, že subjekt údajů je veden v zákonem uvedených zpracováních, může Správce provést výmaz osobních údajů z dokumentů až po uplynutí skartačních lhůt.
4) Správce osobních údajů fyzických osob je povinen postupovat při jejich ochraně ve smyslu Nařízení EU a Rady 2016/679. Jejich zneužití, ztrátu nebo zcizení je povinen bezodkladně nahlásit pověřenci. V případě že pověřenec, po posouzení obsahu a závažnosti dotčených údajů vyhodnotí, že šlo o vážné pochybení, je povinen tuto skutečnost nahlásit Úřadu pro ochranu osobních údajů do 72 hodin a porušení zabezpečení osobních údajů písemně oznámí poškozené osobě.
5) Tato směrnice byla vypracována na základě provedené analýzy ve smyslu závazného Nařízení Evropského parlamentu a Rady EU č. 2016/679 ze dne 27. dubna 2016 a nabývá účinnosti dnem 25. května 2018.

Článek VIII.
Závěrečná ustanovení

Tato směrnice nabývá účinnosti dnem 25. 5. 2018.

Za Správce:

…….
Ing. Karel Pačiska
starosta
Bystřice nad Pernštejnem