Statutární město Brno, městská část Brno-střed

SMĚRNICE O OCHRANĚ A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Směrnice č.: 12
Vydání č.: 1
Účinnost: 25.05.2018

Bc. Petr Štika, MBA, LL.M., v.r.
tajemník ÚMČ Brno-střed

Vydal/schválil: Bc. Petr Štika, MBA, LL.M.
Dne: 21.05.2018
Zpracovatel: Mgr. Vít Křížka, pověřenec pro ochranu osobních údajů

Tato směrnice je závazná pro: Úřad městské části Brno-střed

Projednáno v orgánech: *nejsou*

Osoba pověřená výkladem: Bc. Petr Štika, MBA, LL.M., tajemník ÚMČ BS
Četnost kontroly aktuálnosti: půlročně
Osoba pověřená kontrolou aktuálnosti: Mgr. Jana Plechlová, vedoucí OPO ÚMČ BS

Související vnitřní předpisy:
Pokyn tajemníka o Informačních systémech provozovaných v počítačové síti města Brna, městské části Brno-střed

Historie změn:

Datum	Číslo vydání	Strana	Článek	Stručný popis změny

Odkaz na předešlá vydání:
Nejsou

Související formuláře, záznamy, přílohy a metodiky:
Karta zpracování
Záznamy o činnostech zpracování
Souhlas subjektu údajů se zpracováním osobních údajů
Souhlas subjektu údajů s používáním kontaktních údajů
Oznámení o zpracování osobních údajů (v souvislosti se smlouvou)
Zásady ochrany osobních údajů zaměstnanců
Oznámení o porušení zabezpečení osobních údajů

Zrušovací ustanovení:
Organizační směrnice č. 36/2007 - Ochrana osobních údajů

Příkaz tajemníka č. 2/2010 - Pořizování a uchovávání fotokopií občanských průkazů a cestovních dokladů občanů
Příkaz tajemníka č. 3/2010 - Povinnost zachovávat mlčenlivost o osobních údajích
Příkaz tajemníka č. 4/2010 - Identifikace pracovníků ÚMČ Brno-střed - podatelny, vrátnice
Příkaz tajemníka č. 3/2011 - Stanovisko Úřadu pro ochranu osobních údajů č.1/2010
Příkaz tajemníka č. 3/2013 - Změna organizační směrnice č.36/2007, O ochraně osobních údajů

ČÁST I.
ZÁKLADNÍ USTANOVENÍ

Článek 1
Účel směrnice

(1) Účelem této směrnice je ochrana fyzických osob v souvislosti se zpracováním jejich osobních údajů s ohledem na ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 Smlouvy o fungování Evropské unie.

Článek 2
Správce osobních údajů

(1) Statutární město Brno, městská část Brno-střed je správcem osobních údajů (dále jen „správce“).
(2) Při výkonu přenesené i samostatné působnosti Úřadu městské části Brno-střed (dále jen „ÚMČ BS“) dochází ke zpracovávání osobních údajů občanů, smluvních partnerů, zaměstnanců i dalších osob.
(3) V rámci ÚMČ BS přebírají práva a povinnosti správce osobních údajů jednotlivé odbory nebo jiné organizační útvary (dále jen „útvary“), zajišťující zpracování osobních údajů ve vymezené oblasti.
(4) Ke zpracování osobních údajů dochází rovněž při činnosti Zastupitelstva městské části a jeho výborů, Rady městské části a jejích komisí, starosty a tajemníka.

Článek 3
Pověřenec pro ochranu osobních údajů

(1) Pověřencem pro ochranu osobních údajů (DPO) je Mgr. Vít Křížka, advokát, se sídlem Starobrněnská 690/20, Brno.

Článek 4
Směrnice

(1) Tato směrnice upravuje technická a organizační opatření k zajištění ochrany osobních údajů v souladu s platnou a účinnou legislativou v oblasti ochrany osobních údajů, zejména nikoliv však výlučně zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů a nařízením Evropského parlamentu a Rady (EU) 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 (obecné nařízení o ochraně osobních údajů, GDPR) (dále jen „předpisy na ochranu osobních údajů“), s cílem zajištění zpracování osobních údajů v souladu s touto legislativou a principy, na kterých je vystavěná.
(2) Směrnice je závazná pro všechny zaměstnance ÚMČ BS a zaměstnance organizačních složek MČ BS (dále jen „zaměstnanec“) a oprávněné osoby (jak je tento pojem definován níže).

Článek 5
Vymezení pojmů a zkratek

(1) Pro účely této směrnice se rozumí:
   (a) **osobním údajem** jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě (**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) **osobním údajem zvláštní kategorie** osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

(c) **zpracováním** 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.

(d) **automatizovaným zpracováním** zejména ukládání informací na nosiče dat; provádění logických nebo aritmetických operací s těmito daty, zejména jejich změna, výmaz, vyhledávání nebo rozšiřování uskutečňované zcela nebo zčásti pomocí automatizovaných postupů a provádění archivace informací jejich uložením na archivační paměťová média a v případě potřeby obnovení informací z archivních médií.

(e) **manuálním zpracováním** jakékoliv zpracování s výjimkou zpracování automatizovaného (např. listinná podoba, kartotéky, spisy).

(f) **DPIA** posouzení vlivu na ochranu osobních údajů (anglicky Data Protection Impact Assessment) (jak je tento pojem definován v předpisech na ochranu osobních údajů).

(g) **DPO** pověřenec pro ochranu osobních údajů (anglicky Data Protection Officer) (jak je tento pojem definován v předpisech na ochranu osobních údajů).

(h) **ICT** informační a telekomunikační technologie.

(i) **Informační systém** aplikace zabezpečující zpracování agend v softwarech instalovaných na serverech Odborem informatiky ÚMČ BS.

(i) **oprávněnou osobou** zaměstnanec, který v rámci plnění povinností plynoucích mu z pracovní náplně má přístup k osobním údajům a dále je zpracovává, nebo také osoba, které na základě smluvního vztahu má statutárním městem Brnem, městskou částí Brno-střed povolený přístup k osobním údajům.

(j) **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, chování, místa, kde se nachází, nebo pohybu.

(k) **příjemcem** každý subjekt, kterému jsou osobní údaje zpřístupněny. Za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci; v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského a finančního zájmu České republiky nebo Evropské unie.

(l) **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.

(m) **správcem** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování.
(n) **ÚOOÚ** znamená Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, PSČ 170 00, Praha 7, webové stránky www.uoou.cz.
(o) **zpracovatelem** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

(2) Odkazy na jednotné číslo rovněž zahrnují číslo množné a naopak.

Článek 6
Základní zásady

(1) Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem.
(2) Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely. Osobní údaje musí být omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. Osobní údaje nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.
(3) Osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.
(4) Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.
(5) Osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření s cílem zaručit práva a svobody subjektu údajů.
(6) Osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

ČÁST II.
ÚKONY PŘED ZAPOČETÍM ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Článek 7
Právní titul a účel zpracování

(1) Před započetím zpracování osobních údajů je příslušný útvar povinen vypracovat kartu zpracování a záznamy o činnostech zpracování dle vzorů, které jsou evidovány v Seznamu formulářů a záznamů. Tyto karty a záznamy jsou ponechány na příslušném útvaru a zároveň předány Odboru právnímu a organizačnímu ÚMČ BS a pověřenci pro ochranu osobních údajů.
(2) Účely (důvody) zpracování osobních údajů v jednotlivých agendách vychází ze zvláštních zákonů (zejména při výkonu přenesené působnosti správce), nebo jsou osobní údaje zpracovávány na základě rozhodnutí správce (zejména při výkonu samostatné působnosti správce).
(3) Ke každému účelu zpracování musí být přiřazen právní titul. Právními tituly pro zpracování jsou:
(i) plnění smlouvy, které stranou je subjekt údajů;

(ii) plnění právní povinnosti správce;
(iii) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů;
(iv) splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci;
(v) oprávněný zájem správce a
(vi) souhlas subjektu údajů.

Článek 8
Získání souhlasu

(1) Není-li zpracování osobních údajů nezbytné (i) pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů, (ii) pro splnění právní povinnosti, která se na správce vztahuje, (iii) zpracování není nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, (iv) zpracování není nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým by Společnost byla pověřena, (v) zpracování není nezbytné pro účely oprávněných zájmů správce či třetí strany, zajistí příslušný útvar před zpracováním osobních údajů souhlas subjektu údajů se zpracováním osobních údajů dle vzoru, který je evidován v Seznamu formulářů a záznamů, a tento souhlas (včetně podmínek, za kterých byl udělen) uchovává po celou dobu zpracování osobních údajů tohoto subjektu.
(2) Za souhlas se zpracováním osobních údajů lze považovat rovněž poskytnutí osobních údajů subjekty osobních údajů v listinné nebo v elektronické podobě, pokud je dostatečně zajištěna identita daného subjektu.
(3) Souhlas dětí, tj. osob mladších než 15 let musí být vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k tomuto dítěti.
(4) Udělený souhlas musí být prokazatelný po celou dobu zpracování, včetně všech podmínek, ze kterých je zřetelné k čemu a v jakém znění byl souhlas udělen. V případě, že subjekt údajů souhlas neposkytne, nelze jeho osobní údaje zpracovávat. Každý útvar si vede vlastní evidenci souhlasů.

Článek 9
Souhlas s používáním kontaktních údajů

(1) Pokud ÚMČ BS při výkonu samostatné nebo přenesené působnosti používá kontaktní údaje občana (e-mailovou adresu a telefonní číslo), zajistí příslušný útvar při osobním styku s občanem písemný souhlas s používáním kontaktních údajů dle vzoru, který je evidován v Seznamu formulářů a záznamů, a tento souhlas (včetně podmínek, za kterých byl udělen) uchovává po celou dobu zpracování osobních údajů tohoto subjektu.
(2) Za souhlas se zpracováním kontaktních údajů lze považovat rovněž poskytnutí kontaktních údajů v listinné podobě (zpravidla na formuláři) nebo v elektronické podobě (např. v e-mailu adresovanému správci, a to i bez připojení elektronického podpisu).

Článek 10
Zpracování zvláštních kategorií osobních údajů

(1) Před zpracováním zvláštních kategorií osobních údajů musí být subjekt údajů informován a poučen v rozsahu informační povinnosti dle této směrnice. Zvláštní kategorie osobních údajů mohou být zpracovány pouze s výslovným souhlasem subjektu údajů, kterého se týkají. Za výslovný souhlas lze považovat pouze takové právní jednání, kterým dotčená fyzická osoba výslovně svoluje ke zpracování svých

osobních údajů zvláštních kategorií. Nedá-li tato fyzická osoba výslovný souhlas jejich zpracováním, nelze její osobní údaje zvláštních kategorií zpracovávat.

(2) Poskytnuté osobní údaje zvláštních kategorií jsou pokládány za důvěrné informace a v rámci jejich dalšího zpracování se s nimi mohou seznamovat pouze oprávněné osoby, které tyto údaje potřebují pro plnění svých pracovních povinností.

(3) Specifické podmínky, za nichž je možné zpracovávat osobní údaje zvláštní kategorie bez souhlasu, resp. s dodatečným souhlasem, jsou uvedeny v předpisech o ochraně osobních údajů (viz čl. 9 odst. 2 GDPR).

Článek 11
DPIA

(1) Pokud je pravděpodobné, že určitý druh zpracování osobních údajů bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede ÚMČ BS před zpracováním DPIA.

(2) Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení. V každém takovém případě ÚMČ BS požádá o předchozí konzultaci s ÚOOÚ.

ČÁST III.
INFORMAČNÍ POVINNOST

Článek 12
Sběr údajů

(1) Při shromažďovaní osobních údajů přímo od subjektu údajů musí být subjekt osobních údajů, k němuž se osobní údaje vztahují, informován nejpozději v okamžiku získávání jeho osobních údajů o:

- (i) totožnosti a kontaktních údajích správce;
- (ii) kontaktních údajích pověřence pro ochranu osobních údajů;
- (iii) účelech zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;
- (iv) oprávněných zájmech správce nebo třetí strany v případě, že je zpracování založeno na tomto právním důvodu zpracování;
- (v) případných příjemcích nebo kategoriích příjemců osobních údajů;
- (vi) případném úmyslu správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Evropské komise o odpovídající ochraně nebo, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny;
- (vii) době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
- (viii) existenci práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
- (ix) pokud je zpracování založeno na souhlasu subjektu údajů, existenci práva kdykoli odvolat tento souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
- (x) existenci práva podat stížnost u ÚOOÚ;
- (xi) skutečnosti, 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; a

(xii) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a informacích týkajících se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

(2) Při shromažďovaní osobních údajů jiným způsobem než od subjektu údajů, nemusí být subjekt osobních údajů, k němuž se osobní údaje vztahují, informován, pokud osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství [viz čl. 14 odst. 5 písm. d) GDPR]. V případě, že osobní údaje nemají zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství musí být subjekt osobních údajů informován o skutečnostech uvedených v odst. 1 písm. (i), (ii), (iii), (v) a (vi) tohoto článku a kategoriích dotčených osobních údajů, a to:

(i) v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;

(ii) nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo

(iii) nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

Článek 13
Zásady ochrany osobních údajů

(1) Informační povinnost vůči občanům a třetím osobám plní správce zveřejněním Zásad ochrany osobních údajů na webových stránkách ÚMČ BS.

(2) Informační povinnost vůči smluvním partnerům plní správce předáním Oznámení o zpracování osobních údajů dle vzoru, který je evidován v Seznamu formulářů a záznamů, v okamžiku podpisu smlouvy nebo v průběhu provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.

(3) Informační povinnost vůči zaměstnancům plní správce zveřejněním Zásad ochrany osobních údajů zaměstnanců na intranetu ÚMČ BS.

Článek 14
Formuláře

(1) Jednotlivé útvary průběžně zajišťují kontrolu a revizi všech listinných i elektronických formulářů, na kterých dochází ke sběrů osobních údajů, a to tak, aby na nich bylo zřetelně uvedeno, že dochází ke zpracování osobních údajů v souladu se Zásadami ochrany osobních údajů.

(2) Pokud se na formuláři sbírají osobní údaje třetích osob (odlišných od osoby, která formulář vyplňuje), je nutné na něj uvést poučení o tom, že osoba, která osobní údaje poskytla, o tomto poučí rovněž třetí osobu. Pokud s takovým formulářem pracují osoby, které nejsou vázány služebním tajemstvím nebo zákonem stanovenou povinností mlčenlivosti, je třeba zajistit, aby byly třetí osoby poučeny o tom, že došlo ke zpracování jejich osobních údajů.

ČÁST IV.
VYŘIZOVÁNÍ ŽÁDOSTÍ SUBJEKTŮ ÚDAJŮ

Článek 15
Základní zásady vyřizování žádosti

(1) ÚMČ BS přijímá žádosti subjektů údajů v elektronické nebo v listinné podobě. V případě, že se subjekt údajů obrátí na ÚMČ BS se žádostí ve věci výkonu svých práv v ústní formě telefonicky nebo osobně, příslušný zaměstnanec subjekt údajů informuje o možnosti zformulovat svoji žádost elektronicky nebo písemně, aby mohla být předána podatelně; v případě, že subjekt trvá na vyřízení žádosti telefonicky nebo ústně, žádost bude vyřízena tímto způsobem (v případě nemožnosti identifikovat po telefonu druhou stranu bude žádost zpravidla zamítnuta).
(2) Žádosti mohou být ÚMČ BS zaslané i jí určeným zpracovatelem, odpovědnost za vyřízení takových žádostí má však vždy správce.
(3) Žádosti mohou být ÚMČ BS zaslané i prostřednictvím pověřence pro ochranu osobních údajů. Ten předá žádost podatelně a příslušnému útvaru do 5 pracovních dnů od přijetí žádosti s doporučením vhodného postupu při vyřízení žádosti. Je-li příslušných útvarů více, předává se žádost Odboru právnímu a organizačnímu ÚMČ BS.
(4) ÚMČ BS bude nakládat s přijatou žádostí dle postupu níže v případě, že:
   (i) se žádost týká osobních údajů a/nebo jejich zpracování; nebo
   (ii) v žádosti se uvádí požadavek na výkon práv subjektu údajů dle právních předpisů v oblasti ochrany osobních údajů; nebo
   (iii) se v žádostí uvádí, že je spojena s právními předpisy v oblasti ochrany osobních údajů.

Článek 16
Postup při vyřizování žádosti subjektu údajů

(1) Každá žádost bude vyřízena v následujících krocích:
   1. ověření identity subjektu údajů – aby bylo zajištěno jednání s konkrétní dotčenou osobou,
   2. vyjasnění žádosti a jejího předmětu – v případě, že ze žádosti není zřejmé, čeho se subjekt údajů dožaduje, nebo jsou v žádosti obsažené chybné informace, jejichž správné znění je však nevyhnutné pro její vyřízení, subjekt údajů bude vyzván k jejímu upřesnění,
   3. posouzení žádosti – zda má subjekt údajů právo na výkon daného práva a zda neexistuje výjimka, která by tento výkon znemožňovala,
   4. vyřízení žádosti – buď zamítnutí žádosti, anebo vyhověním žádosti,
   5. předávání rozhodnutí o žádosti pověřenci pro ochranu osobních údajů, který ji zašle žadateli.
(2) Žádost bude zamítnuta, pokud subjekt údajů není oprávněn vykonat požadované právo nebo existuje výjimka, kvůli které tento výkon není možný. V odůvodnění zamítavé odpovědi na žádost musí být uvedeny důvody zamítnutí a informace o možnosti podat stížnost u ÚOOÚ a vyřízení záležitosti soudní cestou.
(3) Žádosti bude vyhověno, pokud je subjekt údajů oprávněn vykonávat svoje právo a neexistuje výjimka, která by mu v tom bránila.
(4) Subjekt údajů musí být informován o krocích, které byly podniknuty v souvislosti s vyřizováním jeho žádosti do 1 měsíce od jejího podání. V případě větší složitosti záležitosti nebo většího počtu žádosti či námitek podaných subjektem údajů během 1 měsíce, může být lhůta pro vyřízení prodloužena o 2 měsíce, o čem bude subjekt údajů

informován, včetně důvodů pro tento odklad. Odpověď bude subjektu údajů podána ve stejné formě, v jaké byla podána jeho žádost, pokud nebude dohodnuto jinak.

(5) Vyřizování žádosti se činí bezplatně. Jsou-li však žádosti subjektem údajů podané zjevně nedůvodně nebo nepřiměřeně, zejména pokud se opakují, může ÚMČ BS účtovat za vyřízení žádosti přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo s učiněním požadovaných úkonů, případně může odmítnou žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti musí být ÚMČ BS schopen doložit.

(6) V případě složité žádosti či při jakýchkoli nejasnostech je zaměstnanec, který žádost vyřizuje, povinen zkonzultovat věc s pověřencem pro ochranu osobních údajů.

Článek 17
Právo na přístup

(1) V obdržené žádosti o uplatnění práva na přístup se identifikuje jeden z následujících předmětů žádosti:
   (i) potvrzení, jestli jsou nebo nejsou ÚMČ BS zpracovávané osobní údaje daného subjektu údajů;
   (ii) informace o tom, jak jsou osobní údaje subjektu údajů zpracovávány; nebo
   (iii) přehled veškerých nebo určitých osobních údajů, které jsou o subjektu údajů zpracovávány.

(2) Toto právo je nepodmíněné a nejsou zde žádné výjimky, takže se žádosti musí vyhovět, přičemž se musí brát ohled na práva a svobody třetích osob, které by mohly být dotčeny poskytnutím vyžádaného přehledu. přehled veškerých nebo určitých osobních údajů, které jsou o subjektu údajů zpracovávány

(3) Pokud je podána žádost o přístup k veškerým osobním údajům, zaměstnanec, který žádost vyřizuje, může vyzvat žadatele, aby žádost specifikoval, nicméně pokud tak žadatel neučiní, je třeba žádost ve lhůtě dle čl. 16 odst. 4 této směrnice vyřídit.

Článek 18
Právo na opravu

(1) Osobní údaje zpracovávané správcem musí být úplné, správné a aktuální. Na základě žádosti subjektu údajů se do všech systémů ÚMČ BS a pověřených zpracovatelů či příjemců vloží opravené nebo doplněné údaje a ty budou použity při všech dalších zpracováních.

(2) Pokud je v žádosti subjektů údajů obsažen také požadavek na omezení zpracování po dobu, než bude korekce údajů a takové opatření je nezbytné pro ochranu práv a svobod subjektu údajů, dojde k přerušení zpracování osobních údajů po dobu, kdy probíhá jejich korekce.

Článek 19
Právo na výmaz (právo být zapomenut)

(1) Subjekt údajů je oprávněn požadovat výmaz jen za určitých podmínek, a to když:
   (i) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;
   (ii) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;
   (iii) subjekt údajů vznese námitku proti zpracování a neexistují žádné převažující oprávněné důvody správce pro zpracování;
   (iv) osobní údaje byly zpracovány protiprávně;

(v) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Evropské unie nebo České republiky; nebo
(vi) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

(2) Každá žádost musí být individuálně posouzena, zda jsou podmínky splněny a zda se neuplatní žádné výjimky, na základě, kterých musí být určité osobní údaje i přes žádost o výmaz zpracovávány (např. k plnění zákonné povinnosti).
(3) V případě, že ÚMČ BS vyhodnotí, že požadované údaje lze vymazat, uvědomí o této skutečnosti i všechny ostatní zpracovatele a zajistí, aby ani tito již předmětné osobní údaje nezpracovávali.

Článek 20
Právo na omezení zpracování

(1) Omezení zpracování je dočasné opatření, o které může být subjektem údajů žádáno v případě:
(i) že zpracování je protiprávní, subjekt dat odmítá výmaz a žádá místo něho omezení;
(ii) aby se aplikovalo během vyřizování žádosti o opravu nebo námitky subjektu údajů proti zpracování (subjekt dat popírá přesnost údajů); a
(iii) jako ochrana proti vymazání osobních údajů, ke kterému by jinak došlo (např. subjekt vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad důvody subjektů údajů).
(2) Za některých podmínek můžou být osobní údaje, kterých zpracování je omezeno, zpracovány pro určité účely, např.: ochrana právních zájmů nebo zpracování se souhlasem subjektu.

Článek 21
Právo vznést námitku

(1) Prvním krokem ke zpracování námitky je zjištění, zda je podávána proti zpracování osobních údajů pro marketingové účely, oprávněné zájmy správce nebo zda jde o zpracování ve veřejném zájmu nebo pro vědecké či statistické účely týkající se jedinečné situace subjektu údajů.
(2) Právo vznést námitku proti zpracování pro účely přímého marketingu je nepodmíněné a námitce musí vždy vyhovět, přičemž není podstatné, na jakém právním důvodu se toto zpracování zakládá.
(3) Každá žádost musí být individuálně posouzena, zda jsou podmínky splněny a zda se neuplatní žádné výjimky.
(4) Po vyhovění žádosti nesmí být osobní údaje používány pro dané účely (marketing, oprávněný zájem, statistika, výzkum) a budou v souladu s principem minimalizace vymazány. Pokud jsou dané osobní údaje zpracovávány pro jiné účely, toto zpracování může probíhat i nadále.

Článek 22
Právo na přenositelnost

(1) Právo na přenositelnost může subjekt údajů uplatnit v případě, že je zpracování založeno na právním důvodu uděleného souhlasu a pro účely uzavření a plnění smlouvy a zároveň když je zpracování prováděno automatizovaně. Výjimkou je zpracování nezbytné ve veřejném zájmu nebo při výkonu veřejné moci.

(2) Osobní údaje (poskytnuty ÚMČ BS subjektem údajů nebo které byly vytvořeny na základě požadavků subjektu údajů) budou poskytnuty ve strojově čitelném formátu (např. XML).
(3) Subjekt údajů může rovněž požádat o předání těchto osobních údajů jinému správci, a to bez souhlasu správce.
(4) Přenos osobních údajů se uskuteční v takové formě, která minimalizuje bezpečnostní rizika (např. za využití šifrování).
(5) Pokud byly vyžádané osobní údaje předány subjektu údajů, oznámení subjektu údajů se podá jen v případě, že došlo k omezením v důsledku např. dopadu na práva třetích subjektů.

Článek 23
Oznámení subjektům ohledně výmazu, opravy nebo omezení zpracování

(1) V případě vyhovění výkonu výše uvedených práv, musí být zpracovatelé a jiní příjemci osobních údajů informováni o jakémkoliv výmazu, opravě nebo omezení zpracování. Zároveň musí být jasně instruováni k podniknutí kroků k danému výmazu, opravě nebo omezení zpracování.

ČÁST V.
TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

Článek 24
Základní bezpečnostní pravidla pro zaměstnance

(1) Zaměstnanci jsou povinni vynaložit veškeré úsilí k tomu, aby nedošlo k porušení zabezpečení osobních údajů, zejména pak musí předcházet neoprávněnému zpřístupnění osobních údajů třetím osobám a ztrátě osobních údajů.
(2) Zaměstnanci jsou povinni při jakýchkoli nejasnostech při zpracování osobních údajů konzultovat danou věc s pověřencem pro ochranu osobních údajů.
(3) Zaměstnanci jsou povinni dodržovat zejména následující bezpečnostní opatření:
   (i) veškeré osobní údaje, podklady, dokumenty nebo jakékoliv jiné materiály a nosiče obsahující osobní údaje uchovávat na chráněných místech a z hlediska techniky a bezpečnosti informací a osobních údajů zabezpečené tak, že je zaručeno, že nedojde k jakémukoliv přístupu neoprávněné třetí osoby k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, či k jejich jinému neoprávněnému zásahu;
   (ii) při zpracování dat, pokud je to technicky a organizačně možné, využívat metodu tzv. pseudonymizace osobních údajů, tzn. neuvádět jména, ani jiné identifikační údaje, např. data narození či rodná čísla, ale naopak využívat jiné náhodně přidělené identifikátory;
   (iii) nesdělovat osobní údaje neoprávněným osobám, a to ani telefonicky ani při osobním jednání, ani jinak neumožnit neoprávněným osobám přístup k osobním údajům, zejména neopouštět prostory, kde se momentálně nachází dokumenty obsahující osobní údaje, pokud jsou zde přítomny třetí osoby;
   (iv) jsou-li dány legitimní účely pro zpřístupnění údajů nebo je-li zpřístupnění právní povinností (např. na základě výzvy exekutora či orgánu činného v trestním řízení), zpřístupnit údaje pouze v přiměřeném rozsahu ve vztahu k účelu zpracování nebo v rozsahu, který stanoví zvláštní právní předpis (občanský soudní řád, exekuční řád, trestní řád);

(v) jsou-li dány legitimní účely pro zveřejnění údajů, zveřejnit údaje pouze v přiměřeném rozsahu ve vztahu k účelu zpracování;
(vi) při zpracovávání osobních údajů využívat pouze schválené programy, formuláře a vzorové dokumenty schválené správcem;
(vii) bezodkladně ohlásit jakékoli porušení zabezpečení ochrany osobních údajů (bezpečnostní incident) Odboru právnímu a organizačnímu.

Článek 25
Identifikační karty

(1) Zaměstnanci jsou povinni používat identifikační karty, jejichž vyhotovení zajišťuje Odbor informatiky ÚMČ BS. Identifikační karty jsou vyhotovovány za účelem usnadnění komunikace veřejnosti s úředními osobami, na čemž je dán veřejný zájem a zároveň jde o oprávněný zájem správce (princip otevřenosti a transparentnost veřejné správy).
(2) O tomto zpracování je taktéž vyhotovena karta zpracování a záznamy o zpracování, a to Odborem informatiky ÚMČ BS.
(3) Zaměstnanci jsou o zpracování osobních údajů v souvislosti s identifikačními kartami informováni prostřednictvím Zásad ochrany osobních údajů zaměstnanců.
(4) Podrobnosti týkající se povinnosti nosit identifikační karty stanoví pracovní řád.

Článek 26
E-mailová korespondence

(1) Zaměstnanci jsou povinni při plnění svých pracovních povinností používat výhradně pracovní e-mailové adresy na doméně brno-stred.cz. Zakazuje se používat osobní e-mailové účty, přeposílání pošty z domény brno-stred.cz na jinou doménu a rovněž použití e-mailového klienta jiného, než kterého stanoví Odbor informatiky ÚMČ BS.
(2) Pokud zaměstnanec očekává delší nepřítomnost v práci z důvodu čerpání dovolené, pracovní neschopnosti či jiné překážky v práci na straně zaměstnance, je povinen vhodným způsobem zajistit vyřizování e-mailové korespondence. Zaměstnanec může udělit souhlas k přístupu ke své e-mailové korespondenci jinému zaměstnanci nastavením přeposílání pošty, popř. nastavit automatickou odpověď s tím, že veškerou komunikaci zvládne včas vyřídit po skončení dovolené či překážky v práci.

Článek 27
Komunikace s orgány samosprávy

(1) Zaměstnanci jsou povinni koncipovat názvy bodů určených k projednání na Zastupitelstvu městské části Brno-střed tak, aby nedošlo k neoprávněnému zpřístupnění či zveřejnění osobních údajů, tj. zejména bez uvedení jmen, příjmení a dalších identifikátorů fyzických osob, neboť program Zastupitelstva městské části Brno-střed je zveřejňován bez další úpravy (anonymizace) na úřední desce a na webových stránkách městské části.
(2) Zaměstnanci jsou povinni formulovat podklady pro Zastupitelstvo městské části Brno-střed, jeho výbory, Radu městské části a její komise či starostu tak, aby nedošlo k neoprávněnému zpřístupnění či zveřejnění osobních údajů, tj. poskytovat pouze nezbytně nutné osobní údaje (s ohledem na zásadu minimalizace osobních údajů). Při předávání dokumentů orgánům samosprávy je třeba zajistit bezpečnost sdělovaných informací.
(3) Zaměstnanci jsou povinni při zveřejňování záměrů obce k dispozici s majetkem podle ustanovení § 39 zákona o obcích postupovat v souladu vyvěšovat buď neadresný záměr

(pouze s údaji o nemovitosti) nebo v případě adresného záměru uvádět (vedle údajů o nemovitosti) pouze iniciály jména a příjmení osoby a obec jejího bydliště.

Článek 28
Zpracovatelé a příjemci

(1) Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

(2) Příjemcem je 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 českým právním řádem (orgány činné v trestním řízení, celní orgány, policejní orgány, …) se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

(3) Pokud příslušný útvar využije ke zpracování zpracovatele, pak je povinen s ním uzavřít písemnou smlouvu o zpracování osobních údajů. Ve smlouvě musí být minimálně uvedeno jaký je předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.

(4) Zpracovatel se dále ve smlouvě zaváže k/ke:
   (i) zpracovávání osobních údajů pouze na základě doložených pokynů správce,
   (ii) zajištění, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
   (iii) přijetí vhodných opatření k zajištění bezpečnosti osobních údajů;
   (iv) dodržení smluvených/zákonných podmínek pro případné zapojení dalšího zpracovatele;
   (v) zohledňování povahy zpracování, tj. že bude správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné,
   (vi) součinnost pro splnění povinnosti správce reagovat na žádosti o výkon práv subjektu údajů;
   (vii) pomoci správci při zajišťování souladu s jeho povinnostmi podle předpisů v oblasti ochrany osobních údajů, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;
   (viii) k tomu, že v osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Evropské unie nebo České republiky nepožaduje uložení daných osobních údajů; a
   (ix) poskytnutí veškerých informací správci potřebných k doložení skutečnosti, že byly splněny povinnosti stanovené v tomto článku, a umožnění auditů, včetně inspekcí, prováděných správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

(5) Při předávání osobních údajů příjemci je třeba zohlednit, zda je takové předání v souladu s účelem zpracování. Pokud je to vhodné, zaváže příslušný útvar příjemce k mlčenlivosti.

Článek 29
Pořizování kopií dokladů

(1) Při výkonu státní správy lze pořizovat kopie občanských průkazů a cestovních dokladů (viz ustanovení § 22b zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů).

(2) Při výkonu samosprávy a samostatné působnosti je pořizování kopií občanských průkazů a cestovních dokladů zakázáno, ledaže je pořizování kopií stanoveno zvláštním právním předpisem nebo mezinárodní smlouvou, kterou je Česká republika vázána.

Článek 30
Agenda ochrany osobních údajů

(1) Za agendu ochrany osobních údajů je odpovědný Odbor právní a organizační ÚMČ BS, který úzce spolupracuje s pověřencem pro ochranu osobních údajů.
(2) Agenda ochrany osobních údajů zahrnuje plnění následujících povinností:
   (i) monitorování změn v předpisech o ochraně osobních údajů, příp. dalších právních předpisů s dopadem do problematiky zpracování osobních údajů;
   (ii) zevšeobecnění poznatků z kontrolní činnosti ÚOOÚ;
   (iii) sledování nových skutečností promítajících se do systému ochrany osobních údajů (např. organizační, personální změny),
   (iv) zahrnutí problematiky ochrany osobních údajů do plánu vzdělávání zaměstnanců správce,
   (v) provedení aktualizace této směrnice při výrazných změnách právních předpisů v oblasti ochrany osobních údajů.

Článek 31
Pověřenec pro ochranu osobních údajů

(1) Pověřenec pro ochranu osobních údajů vykonává tyto úkoly:
   (i) poskytuje informace a poradenství správci, tj. zejména zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle předpisů na ochranu osobních údajů, zejména poradenství v oblasti nařízení GDPR;
   (ii) monitoruje soulad činnosti správce s GDPR a dalšími předpisy na ochranu osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
   (iii) poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 GDPR;
   (iv) spolupracuje s Úřadem pro ochranu osobních údajů a
   (v) působí jako kontaktní místo pro Úřad pro ochranu osobních údajů v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 GDPR, a případně vedení konzultací v jakékoli jiné věci.
(2) Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Článek 32
Závazek důvěrnosti a mlčenlivosti

(1) Zaměstnanci jsou povinni zachovávat mlčenlivost o všech osobních údajích (zejména obsažených v dokumentech, souborech, v databázích či v informačních systémech) a o všech dalších skutečnostech, o nichž se dozvěděli v souvislosti s výkonem práce pro správce. O těchto skutečnostech jsou povinni zachovávat mlčenlivost i po skončení pracovněprávního vztahu.
(2) Pokud zaměstnanec vědomě poruší povinnost mlčenlivosti, bude to zaměstnavatel považovat za porušení pracovní kázně zvlášť hrubým způsobem a může se zaměstnancem okamžitě rozvázat pracovní poměr podle § 55 odst. 1 písm. b) zákoníku práce.

(3) Jestliže zaměstnanec, který byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly shromážděné v souvislosti s výkonem veřejné moci, vystavuje se nebezpečí trestního stíhání pro trestný čin dle § 180 zákona č. 40/2009 Sb., trestního zákoníku. Stejnému postihu se vystavuje zaměstnanec, který byť i z nedbalosti, poruší povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého zaměstnání.

Článek 33
Pravidla pro zaměstnance využívající ICT prostředky

(1) Zaměstnanci využívající ICT prostředky, které jim byly svěřeny správcem, je mohou využívat pouze k výkonu svých pracovních povinností dle pravidel obsažených v pokynu tajemníka o Informačních systémech provozovaných v počítačové síti města Brna, městské části Brno-střed, zejména s pravidly v provozním řádu.
(2) Zaměstnanci mají povinnost chránit svěřené ICT prostředky před ztrátou, poškozením, zničením či zcizením. Zejména jsou povinni uzamykat místnosti s ICT prostředky při nepřítomnosti a přiměřeným způsobem chránit přidělené mobilní ICT prostředky.
(3) V případě, že zaměstnanec ICT prostředek nemá pod přímou kontrolou (např. při opuštění kanceláře), musí používat základní ochranné prostředky, tj. např. software „uzamykání“ ICT prostředku, nebo jeho vypínání.

Článek 34
Pravidla řízení přístupu k osobním údajům

(1) Řízení přístupu k prostředkům ICT je prováděno za uplatnění následujících principů, které se uplatňují jak pro zaměstnance, tak pro externí subjekty jako obchodní partnery a dodavatele, např. zajišťující služby pro správce na základě smluvního vztahu:
   (i) princip minimálního oprávnění, tzn. přidělení pouze takových oprávnění, která jsou nezbytná k plnění jeho pracovních/smluvních povinností;
   (ii) princip periodického přezkoumávání přístupových oprávnění;
   (iii) princip revize a změny přístupových oprávnění při změně pracovní pozice či pracovní náplně zaměstnance či změně smluvního vztahu s jinými subjekty;
   (iv) princip odebrání všech přístupových oprávnění při ukončení pracovního/smluvního vztahu.
(2) V případě sporu o přístup k prostředkům ICT, vč. sporu o jednotlivá oprávnění, jsou zaměstnanci povinni obrátit se na nejbližšího společného nadřízeného zaměstnance, který spor rozhodne. V konečné instanci rozhoduje tajemník ÚMČ BS.

ČÁST VII.
BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

Článek 35
Definice hlavních bezpečnostních rizik

(1) Mezi hlavní bezpečnostní rizika, které hrozí při zpracování osobních údajů v rámci ÚMČ BS patří:
   (i) přístup neoprávněných osob k osobním údajům;
   (ii) zničení nebo zneužití technických prostředků;
   (iii) zneužití záznamů ohledně osobních údajů oprávněnými osobami a

(iv) živelní událost.

Článek 36
Porušení zabezpečení osobních údajů (bezpečnostní incidenty)

(1) Porušením zabezpečení osobních údajů (bezpečnostním incidentem) se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
(2) Oznámení o bezpečnostních incidentech přijímá Odbor právní a organizační ÚMČ BS.
(3) Všechny bezpečnostní incidenty jsou následně vyhodnoceny s cílem určit příčinu výskytu incidentu a přijmout nápravné opatření.
(4) Postup a opatření ke zvládání bezpečnostního incidentu jsou průběžně dokumentována, veškeré dokumentované informace k bezpečnostnímu incidentu jsou uchovávány na Odboru právním a organizačním ÚMČ BS.
(5) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

Článek 37
Postup při řešení bezpečnostního incidentu

(1) Řešení bezpečnostního incidentu zahrnuje následující činnosti:
   (i) bezodkladné oznámení incidentu např. e-mailem, telefonicky či ústně Odboru právnímu a organizačnímu ÚMČ BS, který jej zaeviduje v informačním systému ATTIS;
   (ii) Odbor právní a organizační ÚMČ BS provede prvotní posouzení a prověření incidentu, jeho kategorizaci, posouzení incidentu a jeho dopadů, stanoví míru závažnosti incidentu; v případě potřeby zkontaktuje pověřence pro ochranu osobních údajů a tajemníka ÚMČ BS;
   (iii) Odbor právní a organizační ÚMČ BS navrhne přijetí opatření ke zmírnění či eliminaci dopadů incidentu dle odhadnuté závažnosti incidentu; tímto krokem může Odbor právní a organizační ÚMČ BS pověřit jiné útvary dle jejich specializace (např. Odbor informatiky ÚMČ BS v případě porušení bezpečnosti ICT);
   (iv) přijetí okamžitých protiopatření k eliminaci incidentu a zabránění šíření jeho dopadů dle návrhu příslušných útvarů;
   (v) Odbor právní a organizační ÚMČ BS ve spolupráci s pověřencem pro ochranu osobních údajů provede analýzu a vyhodnocení příčin vzniku incidentu, posouzení slabého místa zabezpečení osobních údajů a návrh opatření ke zlepšení do budoucna.
(2) Při kategorizaci bezpečnostních incidentů se zohlední:
   (i) důležitost dotčených osobních údajů,
   (ii) dopady na výkon státní správy a samosprávy,
   (iii) předpokládané škody a jiné dopady na práva a povinnosti subjektů údajů.
(3) Pro potřeby zvládání bezpečnostních incidentů se incidenty dělí do následujících kategorií:
   (i) kategorie 1 (méně závažný bezpečnostní incident) – dochází k méně významnému narušení bezpečnosti osobních údajů; musí být zamezeno další šíření bezpečnostního incidentu – v systému ATISS bude vyznačena priorita nízká;

(ii) kategorie 2 (závažný bezpečnostní incident) – je narušena bezpečnost osobních údajů; jeho řešení vyžaduje neprodlený zásah k zamezení dalšímu šíření bezpečnostního incidentu – v systému ATISS bude vyznačena priorita střední;
(iii) kategorie 3 (velmi závažný bezpečnostní incident) – je významně narušena bezpečnost osobních údajů; řešení vyžaduje neprodlený zásah obsluhy, všemi dostupnými prostředky musí být zabráněno dalšímu šíření bezpečnostního incidentu – v systému ATISS bude vyznačena priorita vysoká.

Článek 38
Oznamování případů porušení zabezpečení osobních údajů

(1) Druh, způsob a lhůty podávání oznámení závisí na tom, do které kategorie bezpečnostní incident spadá:
(i) kategorie 1: žádné oznámení není nutné;
(ii) kategorie 2: v případě porušení zabezpečení osobních údajů je správce povinen oznámit bez zbytečného odkladu, a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, toto porušení Úřadu pro ochranu osobních údajů, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob; nebo
(iii) kategorie 3: správce musí oznámit porušení zabezpečení osobních údajů bez zbytečného odkladu rovněž subjektu údajů.
(2) Oznámení o porušení zabezpečení osobních údajů musí být vyhotoveno v souladu se vzorem, který je evidován v Seznamu formulářů a záznamů.
(3) Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
(i) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
(ii) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
(iii) vyžadovalo by to nepřiměřené úsilí; v takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

ČÁST VIII.
PŘEDÁNÍ OSOBNÍCH ÚDAJŮ DO JINÝCH ZEMÍ

Článek 39
Předání osobních údajů do jiných zemí

(1) V případě předání osobních údaj do členských států Evropského hospodářského prostoru není potřeba realizovat žádná dodatečná opatření.
(2) Předávání osobních údajů do třetích zemí může být založeno na základě mezinárodní smlouvy, příp. na základě rozhodnutí orgánů Evropské unie. Aktuální podmínky pro takové předávání, které jsou dodržovány, jsou uvedeny na webových stránkách Úřadu pro ochranu osobních údajů.

ČÁST X.
KAMEROVÉ SYSTÉMY

Článek 40
Provoz kamerových systémů

(1) Ve vnějších a vnitřních prostorech budov ÚMČ BS a budov ve vlastnictví správce jsou instalovány kamerové systémy se záznamovým zařízením. Účelem instalace těchto kamerových systémů je ochrana majetku, bezpečnosti a dalších oprávněných zájmů správce, jeho zaměstnanců i dalších osob, nacházejících se v těchto budovách.
(2) O tomto zpracování jsou taktéž vyhotoveny karty zpracování a záznamy o zpracování. Tyto karty a záznamy pořizuje Odbor informatiky ÚMČ BS.
(3) Subjekty údajů (zaměstnanci, občané, ...) jsou o kamerovém systému informováni formou piktogramu, kde je uveden odkaz na Zásady ochrany osobních údajů, kde jsou uvedeny podrobnější informace o právech, které mohou subjekty údajů uplatňovat, a rovněž seznam všech kamer.
(4) Snímané záběry jsou uchovávány v záznamových zařízeních po dobu nejvýše 3 dnů. Po této době jsou zaznamenaná data automaticky přemazána novým zápisem.
(5) Kamerové systémy nejsou napojeny na žádnou databázi operující s osobními údaji. Záznamy z kamerových systémů budou využity v souladu s účelem jejich instalace, a to v případě vnitřního šetření identifikovaného incidentu, nebo budou předány na vyžádání orgánů činných v trestním řízení jako důkazní materiál vyšetřování.

Článek 41
Provoz kamerových systémů v bytových domech

(1) Ve vnějších a vnitřních prostorech bytových domů ve vlastnictví správce mohou být instalovány kamerové systémy se záznamovým zařízením. Účelem instalace těchto kamerových systémů je ochrana majetku, bezpečnosti a dalších oprávněných zájmů správce a obyvatel těchto domů.
(2) O tomto zpracování jsou taktéž vyhotoveny karty zpracování a záznamy o zpracování. Tyto karty a záznamy pořizuje Správa nemovitostí městské části Brno-střed, která rovněž zajistí uzavření zpracovatelských smluv v případě, že provoz kamerového systému zajišťuje třetí osoba.
(3) Subjekty údajů (nájemci, návštěvníci domů, ...) jsou o kamerovém systému informováni formou piktogramu, kde je uveden odkaz na Zásady ochrany osobních údajů, kde jsou uvedeny podrobnější informace o právech, které mohou subjekty údajů uplatňovat, a rovněž seznam všech kamer.
(4) Snímané záběry jsou uchovávány v záznamových zařízeních po dobu nejvýše 5 dnů v případě, že dochází k monitorování prostor, kde dochází ke vstupům do obydlí (vstup do domu, chodby se vstupy do jednotlivých bytů) a po dobu nejvýše 10 dnů v případě, že dochází k monitorování zbylých prostor (garáže, parkovací místa, ostatní společné prostory, …). Po této době jsou zaznamenaná data automaticky přemazána novým zápisem.
(5) Kamerové systémy nejsou napojeny na žádnou databázi operující s osobními údaji. Záznamy z kamerových systémů budou využity v souladu s účelem jejich instalace, a to v případě vnitřního šetření identifikovaného incidentu, nebo budou předány na vyžádání orgánů činných v trestním řízení jako důkazní materiál vyšetřování.

Článek 42
Provoz docházkového systému

(1) Na pracovištích ÚMČ BS je instalován elektronický docházkový systém včetně kamerového systému, který u docházkového systému pořídí fotografii každé osoby provádějící záznam v docházkovém systému za účelem ztotožnění zaměstnance a osoby provádějící vyznačení. Tento kamerový systém je provozován se souhlasem zaměstnanců.
(2) Se souhlasem zaměstnance může být veřejnost prostřednictvím webových stránek ÚMČ BS informována o přítomnosti konkrétního zaměstnance na pracovišti.
(3) O tomto zpracování je taktéž vyhotovena karta zpracování a záznamy o zpracování, a to Odborem právním a organizačním ÚMČ BS.
(4) Zaměstnanci jsou o kamerovém systému informováni prostřednictvím Zásad ochrany osobních údajů zaměstnanců.
(5) Snímané záběry jsou uchovávány v záznamových zařízeních po dobu nejvýše 3 dnů.