Chomutov	**SMĚRNICE RM**
Číslo dokumentu	**2023 – 31**
Autor dokumentu	Ing. Jarmila Mravcová, MPA
Správce dokumentu	Mgr. David Kuhn
Schvalovatel dokumentu	Tajemník MMCH
Účinnost	15.01.2024

SMĚRNICE PRO ZABEZPEČENÍ OCHRANY OSOBNÍCH ÚDAJŮ

Anotace

Tato směrnice stanoví základní pravidla a postupy pro zabezpečení ochrany osobních údajů fyzických osob v rámci působnosti statutárního města Chomutova (dále jen „SMCH“) a Magistrátu města Chomutova (dále jen MMCH), dle zákona č. 110/2019 Sb., o zpracování osobních údajů, dalších zvláštních zákonů a nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů, dále jen jako „Obecné nařízení“ nebo „GDPR“)

Počet stan	27
Počet příloh	8
Podpis autora	**Ing. Jarmila Mravcová** Digitální podpis: 05.01.2024 12:01
Datum vydání a podpis vydavatele	**Ing. Robert Plechatý MPA** Digitální podpis: 08.01.2024 08:23

OBSAH

ZMĚNOVÝ LIST

Datum účinnosti	Změněná část	Popis změny
15.01.2024	Číslo směrnice	Změna čísla směrnice v souladu s novým systémem číslování vnitřních předpisů účinným od 02.01.2023 Původní číslo směrnice: 028-12-04 Nové číslo směrnice: 2023 - 31
	Celý text směrnice	Úprava vzhledu dokumentu v souladu se směrnicí č. 2023 - 01 – Tvorba vnitřních dokumentů
	Celý text směrnice	Promítnutí nového zákona č. 110/2019 Sb., o zpracování osobních údajů

KAPITOLA 1
ÚČEL A ROZSAH PŮSOBNOSTI

1) Tato směrnice stanovuje práva a povinnosti při zpracování a ochraně osobních údajů, upravuje procesní a organizační opatření k zajištění povinností vyplývajících z legislativního rámce pro zabezpečení ochrany osobních údajů.

2) Směrnice se vydává v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákonem č. 110/2019 Sb., o zpracování osobních údajů.

3) Směrnice upravuje povinnosti SMCH a jeho zaměstnanců při provádění automatizovaného i neautomatizovaného zpracování osobních údajů. Směrnice se nevztahuje na nahodilé, neúmyslné získání osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

4) SMCH je v postavení Správce osobních údajů a z tohoto důvodu zodpovídá za zpracování získávaných údajů v souladu s platnou legislativou. SMCH se zavazuje shromažďovat a vést pouze takové osobní údaje o subjektech, které umožňují poskytovat bezpečné, odborné a kvalitní služby. Pro práci s těmito osobními údaji byl vytvořen příslušný systém práce pro všechny personální úrovně, byl definován soubor osobních údajů, jejichž získávání je pro zajištění poskytování kvalitních, odborných a bezpečných služeb klientům nezbytné, dále bylo přesně vymezeno, k jakému účelu budou konkrétní osobní údaje využívány a také byla posouzena možná rizika spojená se zajištěním bezpečnosti osobních údajů a jejich správou. V organizačním a pracovním řádu byly ustanoveny role/pozice odpovědné za dodržování legislativní podmínek v oblasti ochrany osobních údajů.

5) Tato směrnice je závazná pro všechny osoby v zaměstnaneckém či obdobném poměru ke statutárnímu městu Chomutov, které přichází do styku s osobními údaji.

KAPITOLA 2
POUŽITÉ ZKRATKY A ZÁSTUPNÁ OZNAČENÍ

DPIA	posouzení vlivu na ochranu osobních údajů ((Data Protection Impact Assessment))
IP adresa	identifikace zařízení v počítačové síti
DPO	pověřenec pro ochranu osobních údajů
Legislativní rámec	**z**ákony a nařízení - zákon č. 110/2019 Sb., o zpracování osobních údajů - nařízení 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)

- zákon č. 89/2012 Sb., Občanský zákoník

MAC	jednoznačný identifikátor síťového zařízení (tzv. fyzická adresa)
Obecné nařízení	Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Garant agendy	osoba odpovědná za agendu zpracování osobních údajů na odboru nebo v organizační složce – vedoucí odboru, vedoucí organizační složky, ředitel Městské policie
OIT	odbor informačních technologií, odpovědný za zajištění informační bezpečnosti
OÚ	osobní údaje
SÚ	subjekt údajů
Dozorový úřad/Úřad	Úřad pro ochranu osobních údajů (též ÚOOÚ)
Provoz	oddělení provozu budov
SMCH	statutární město Chomutov

KAPITOLA 3
VÝKLAD POJMŮ

1) **Osobní údaje** - veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen "subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

   Konkrétní osobu lze identifikovat zejména různou kombinací osobních údajů.

   Příklad osobních údajů, resp. údajů pro kombinace osobních údajů, které jsou zpracovávány SMCH:
   - jméno
   - příjmení
   - podpis
   - datum a místo narození
   - rodné číslo
   - pohlaví
   - trvalé bydliště
   - soukromé telefonní číslo
   - firemní telefonní číslo
   - soukromý email
   - firemní email
   - číslo občanského průkazu

- číslo pasu
- číslo řidičského průkazu
- certifikát pro elektronický podpis
- údaje v osobní evidenci
- údaje ve mzdové evidenci
- údaje pro zdravotní pojišťovnu
- údaje pro splnění kvalifikačních předpokladů
- údaje v životopise (v období mezi podáním přihlášky do výběrového řízení a uzavřením či neuzavřením pracovního poměru)
- údaje v záznamu o dopravní nehodě služebního vozidla
- kamerové záznamy, fotografie
- IP adresy, MAC adresy.

2) **Zvláštní kategorie osobních** údajů - zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají 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. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby. Dříve označováno jako tzv. citlivé osobní údaje.

   Příklady zvláštní kategorie osobních údajů obvykle se vyskytujících v SMCH:

   - údaje o příslušnosti k odborové organizaci (srážky ze mzdy – příspěvky).

3) **Subjekt údajů** - fyzická osoba, kterou lze přímo či nepřímo identifikovat pomocí osobních údajů.

4) **Správce** - právnická osoba, která určuje účely a prostředky zpracování osobních údajů. Správcem osobních údajů je SMCH.

5) **Zpracovatel** – fyzická (OSVČ) nebo právnická osoba, která zpracovává osobní údaje pro Správce.

6) **Likvidace osobních údajů** - je fyzické zničení nosiče osobních údajů, jejich fyzické vymazání nebo trvalé vyloučení z dalšího zpracování.

7) **Zpracování** - 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.

8) **Porušení 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.

9) **Dozorový úřad** - Úřad pro ochranu osobních údajů.

10) **Dokument** – fyzický (papírový) dokument, nebo elektronický objekt obsahující data s osobními údaji.

11) **Kopie dokumentu** – scan, fotokopie (apod.) fyzického dokumentu, anebo datová kopie el. souboru.

12) **Zabezpečené úložiště** - datový prostor jako je centrální diskové pole, pevný disk počítačů, spisový uzel, spisovna.

13) **Evidence úložišť OÚ** - evidence všech úložišť, kde je možné ukládat OÚ, např.:

    - centrální datové úložiště a informační systémy
    - pevný disk osobního počítače
    - přenosné úložiště (flash disk, externí pevný disk)
    - úložiště přenosných zařízení (notebook, tablet, mobilní telefon)
    - úložiště fyzických dokumentů (spisové uzly, spisovny, jednotlivé kanceláře)
    - evidence úložišť bude vedena na každém odboru a zodpovědnost za její správnost ponese garant agendy.

14) **Datové inventurní záznamy** - obsahují informace o jednotlivých zpracování OÚ v SMCH v rozsahu nezbytném pro generování záznamů o zpracování, vytváření podkladů pro rizikovou analýzu a podkladů pro rozhodování o nutnosti provedení DPIA. Vzor datového inventurního záznamu je přílohou č. 1 této směrnice.

15) **Záznamy o činnostech zpracování OÚ** - obsahují informace o Správci a Pověřenci, o účelu zpracování, popis kategorií subjektů údajů a kategorií OÚ, kategorie příjemců, lhůty pro výmaz a technické a organizační bezpečnostní opatření. Vzor záznamu je přílohou číslo 2 směrnice.

16) **Evidence požadavků subjektu údajů** - obsahuje záznamy o požadavcích subjektu údajů na přístup k OÚ, opravu OÚ, výmaz OÚ, omezení zpracování a vznesení námitky včetně informace o tom, jak byly tyto požadavky vypořádány. Vzor evidence požadavků subjektu údajů je přílohou č. 3 směrnice.

17) **Evidence porušení zabezpečení OÚ** – obsahuje dokumentaci veškerých případů porušení zabezpečení osobních údajů, přičemž jsou uvedeny skutečnosti, které se týkají daných porušení, jejich účinky a přijatá nápravná opatření. Vzor evidence porušení zabezpečení OÚ je přílohou č. 4 směrnice.

18) **Evidence potenciálních bezpečnostních incidentů** - obsahuje záznamy o skutečnostech, které by mohly způsobit porušení zabezpečení OÚ, přestože k porušení nedošlo nebo se v dané době neprojevilo. Potenciální bezpečnostní incidenty se neohlašují dozorovému úřadu. Vzor evidence potenciálních bezpečnostních incidentů je přílohou č. 5 této směrnice.

KAPITOLA 4
VYBRANÉ OBECNÉ PODMÍNKY PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Článek 1
ZÁSADY OSOBNÍCH ÚDAJŮ

OÚ musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“)

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný („účelové omezení“)

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“)

d) 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 („přesnost“)

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány („omezené uložení“)

f) 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 („integrita a důvěrnost“).

Článek 2
ZÁKONNOST ZPRACOVÁNÍ

Zpracování OÚ je zákonné, pokud je splněna alespoň jedna z těchto podmínek:

a) subjekt údajů udělil **souhlas** se zpracováním svých OÚ pro jeden či více konkrétních účelů (čl. 6 odst. 1 písm. a) Obecného nařízení)

b) zpracování je nezbytné pro **splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů (čl. 6 odst. 1 písm. b) Obecného nařízení)

c) zpracování je nezbytné pro **splnění právní povinnosti**, která se na Správce vztahuje (čl. 6 odst. 1 písm. c) Obecného nařízení)

d) zpracování je nezbytné pro **ochranu životně důležitých zájmů subjektu** údajů nebo jiné fyzické osoby (čl. 6 odst.1 písm. d) Obecného nařízení)

e) zpracování je nezbytné pro splnění úkolu prováděného **ve veřejném zájmu** nebo **při výkonu veřejné moci**, kterým je pověřen Správce (čl. 6 odst. 1 písm. e) Obecného nařízení)

f) zpracování je nezbytné pro účely **oprávněných zájmů** příslušného Správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě (čl. 6 odst. 1 písm. f) Obecného nařízení).

Článek 3
SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

1) Souhlas musí být svobodným, konkrétním (pro konkrétní účel zpracování), informovaným a jednoznačným projevem vůle subjektu údajů, který jím dává své svolení ke zpracování svých osobních údajů.

2) Subjekt údajů musí být před udělením souhlasu informován o všech skutečnostech zpracování, zejména o SMCH jako Správci, účelech zpracování, o operacích zpracování a o možnosti kdykoli odvolat souhlas, nikoli však se zpětnými účinky.

3) Souhlas musí být udělen v písemné formě, a to buď v listinné, nebo v elektronické podobě.

4) Pokud je od Subjektu údajů nutné získat Souhlas se zpracováním, musí se tak stát za pomoci samostatného dokumentu (v listinné, nebo elektronické podobě).

5) Subjekt údajů je oprávněn jím udělený souhlas kdykoli odvolat. Odvolat souhlas musí být stejně snadné jako jej poskytnout. V případě, že SMCH bude doručeno odvolání souhlasu, je SMCH povinno postupovat v souladu s postupy uvedenými v této směrnici.

6) V případě, že subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování, SMCH je povinno provést likvidaci osobních údajů, které se daného subjektu údajů týkají.

7) Za SMCH eviduje informace o uděleném souhlasu každý jednotlivý garant agendy, který souhlas požaduje, a to v následujícím rozsahu (viz příloha č. 6 této směrnice):

   - kdo a kdy souhlas udělil
   - rozsah informací poskytnutých subjektu údajů před udělením souhlasu
   - forma udělení souhlasu.

8) V případě, že subjekt údajů souhlas odvolal, je součástí evidence též údaj o odvolání souhlasu a o datu odvolání souhlasu.

9) Udělený souhlas je platný pouze pro operace zpracování, které jsou nezbytné a přiměřené k naplnění účelu, pro který byl souhlas udělen.

10) Souhlas se zpracováním osobních údajů dítěte mladšího 15 let v souvislosti se službami informační společnosti je platný pouze v případě, že je vyjádřen nebo schválen jeho zákonným zástupcem.

Článek 4
ZPRACOVÁNÍ ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ

SMCH smí zpracovávat zvláštní kategorie osobních údajů pouze v případech, kdy jde o některý z případů vymezených ve čl. 9 odst. 2 nařízení GDPR, zejména:

a) subjekt údajů udělil výslovný souhlas se zpracováním zvláštních osobních údajů pro jeden či více konkrétních účelů, nebo

b) zpracování je nezbytné pro účely plnění povinností vyplývajících ze smlouvy mezi subjektem a SMCH

c) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů (čl. 9 odst. 2 písm. e) Obecného nařízení)

d) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického významu nebo pro statistické účely, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu OÚ a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů (čl. 9 odst. 2 písm. *j) Obecného nařízení)*.

Článek 5
OPRÁVNĚNÝ ZÁJEM SMCH

1) SMCH je oprávněno zpracovávat osobní údaje subjektu údajů v případě, je-li zpracování nezbytné pro účely plnění oprávněných zájmů SMCH či třetí osoby.

2) Oprávněným zájem SMCH může být např. ochrana před zneužitím služeb, ochrana majetkových zájmů, zajištění bezpečnosti sítě a informací a z dalších důvodů.

3) V každém jednotlivém případě, kdy má dojít ke zpracování osobních údajů na základě oprávněného zájmu, je nutné stanovit oprávněný zájem a dále posoudit:

   a) oprávněnost stanoveného zájmu, tedy zda je stanovený zájem legální a dostatečně specifický a zda jde o skutečný zájem SMCH

   b) nezbytnost zamýšleného zpracování osobních údajů pro účely stanoveného zájmu, zda je v rovnováze oprávněný zájem SMCH a práva subjektu údajů

   c) zda nad stanoveným zájmem SMCH nepřevažují zájmy nebo základní práva a svobody subjektu údajů, včetně posouzení případného přijetí záruk k ochraně práv a svobod subjektů údajů.

4) V případě, že jsou splněny všechny výše uvedené požadavky, smí být v rámci SMCH zahájeno zpracování osobních údajů z důvodu oprávněného zájmu.

Článek 6
ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

1) Správce vede Záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují minimálně tyto informace:
   - jméno a kontaktní údaje Správce a případného společného Správce, zástupce Správce a Pověřence pro ochranu OÚ
   - účely zpracování
   - popis kategorií subjektů údajů a kategorií osobních údajů
   - kategorie příjemců OÚ, kterým byli nebo budou OÚ zpřístupněny
   - je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů
   - je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.
2) Záznamy se vyhotovují písemně, buď v listinné, nebo elektronické verzi. Pro každý účel zpracování OÚ musí být vypracován a veden záznam o činnosti zpracování viz Příloha č. 2.
3) Za věcnou správnost jednotlivých záznamů o činnostech zpracování je odpovědný příslušný garant agendy, v jehož organizačním útvaru probíhá zpracování OÚ, při současném zohlednění zásad zpracování OÚ dle kapitoly 4, článku 1 této směrnice.
4) Garant agendy vede evidenci všech záznamů o činnostech zpracování na příslušném odboru, za celé SMCH vede evidenci Pověřenec. Tato evidence bude vedena v elektronické podobě ve sdílené složce na centrálním datovém úložišti, kam budou mít přístup pouze Pověřenec a tajemník MMCH v plném rozsahu a do složek týkajících se jednotlivých odborů bude mít přístup rovněž garant agendy příslušného odboru.
5) Tajemník MMCH, ve spolupráci s Pověřencem zajišťuje, aby Záznamy o činnostech zpracování byly k dispozici v aktuální formě (elektronické a písemné, nebo jen písemné).
6) Kontrola a aktualizace jednotlivých záznamů o činnostech zpracování se provádí 1x ročně, nejpozději však k 20.12. kalendářního roku. Tajemník MMCH vyzve odpovědné garanty agendy k ověření jejich správnosti, aktuálnosti a případnému doplnění, včetně stanovení příslušných lhůt pro aktualizaci.

Článek 7
POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DPIA)

Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, mít za následek vysoké riziko pro práva a svobody fyzických osob, provede Správce před zpracováním DPIA.

DPIA je nutné zejména v těchto případech:

a) 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

b) rozsáhlé zpracování zvláštních kategorií OÚ nebo OÚ týkajících se rozsudků v trestních věcech a trestných činů

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Článek 8
ZABEZPEČENÍ ZPRACOVÁNÍ

1) S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou Správce a případní Zpracovatelé vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

   a) pseudonymizace a šifrování OÚ

   b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování

   c) schopnosti obnovit dostupnost OÚ a přístup k nim včas v případě fyzických či technických incidentů

   d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2) Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných OÚ, nebo neoprávněný přístup k nim.

3) Pověřenec zajistí zpracování a evidování přijatých a provedených technických a organizačních opatření k zajištění ochrany osobních údajů v souladu s nařízením a zvláštními a interními předpisy. Pověřenec dále posuzuje, zda bude docházet k předání osobních údajů třetím osobám a zda jsou splněny všechny podmínky předání v souladu s nařízením a touto směrnicí.

4) OIT zajistí, že užívat systémy pro automatizované zpracování osobních údajů mohou pouze oprávněné osoby, a to pouze v rozsahu odpovídajícímu jejich oprávnění, že o přístupu do těchto systémů budou vedeny elektronické záznamy o přístupu k osobním údajům a provedených úkonech a rovněž zabrání neoprávněnému přístupu k nosičům informací.

Článek 9
UZAVÍRÁNÍ SMLUV SE ZPRACOVATELI OÚ

1) Pro zpracování OÚ využije Správce pouze ty Zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Obecného nařízení a aby byla zajištěna dostatečná ochrana práv subjektu údajů.

2) Zpracovatel nezapojí do zpracování žádného dalšího Zpracovatele bez předchozího písemného povolení Správce.

3) Zpracování Zpracovatelem se řídí smlouvou, která zavazuje Zpracovatele vůči Správci a v níž je stanoven předmět a doba trvání, povaha a účel zpracování, typ OÚ a kategorie subjektů údajů, povinnosti a práva Správce. Tato smlouva nebo jiný právní akt stanoví zejména, že Zpracovatel:

   a) zpracovává osobní údaje pouze na základě doložených pokynů Správce,

   b) zajišťuje, aby se osoby oprávněné zpracovávat OÚ zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,

   c) zajistí zabezpečení zpracování zejména:

      - pseudonymizací a šifrováním OÚ
      - schopností zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
      - schopností obnovit dostupnost údajů a přístup k nim v případě fyzických či technických incidentů
      - procesem pravidelného testování, posuzování a hodnocení účinnosti zavedených opatření.

   d) poskytuje součinnost při zajištění souladu s následujícími povinnostmi:

      - zabezpečení zpracování
      - ohlašování případů porušení zabezpečení OÚ dozorovému úřadu
      - oznamování případů porušení zabezpečení OÚ subjektu údajů
      - posouzení vlivu na ochranu OÚ
      - předchozí konzultace (před zpracováním s dozorovým úřadem)
      - v souladu s rozhodnutím Správce všechny OÚ buď vymaže, anebo je vrátí Správci po ukončení poskytování služeb spojených se zpracováním a vymaže existující kopie, pokud legislativa nepožaduje uložení daných OÚ
      - poskytne Správci veškeré informace potřebné k doložení toho, že byly splněny všechny povinnosti.

Článek 10
PRÁVO SUBJEKTU ÚDAJŮ NA PŘÍSTUP K OÚ

1) Subjekt údajů má právo získat od Správce potvrzení, zda OÚ, které se ho týkají, jsou či nejsou zpracovávány, a pokud zpracovávány jsou, má právo získat přístup k těmto OÚ a k následujícím informacím:

   a) účely zpracování

   b) kategorie dotčených OÚ

   c) příjemci nebo kategorie příjemců, kterým byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích

d) plánovaná doba, po kterou budou OÚ uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby

e) existence práva požadovat od Správce opravu nebo výmaz OÚ týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování

f) právo podat stížnost u dozorového úřadu

g) veškeré dostupné informace o zdroji OÚ, pokud nejsou získány od subjektu údajů

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a informace týkající se použitého postupu.

2) Správce poskytne kopii zpracovávaných OÚ zdarma. Za další kopie na žádost subjektu údajů může Správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

3) Právem získat kopii nesmí být dotčena práva a svobody jiných osob.

Článek 11
PRÁVO SUBJEKTU NA OPRAVU

Subjekt údajů má právo na to, aby Správce bez zbytečného odkladu opravil nepřesné OÚ, které se ho týkají. Opravu jména či příjmení, případně čísla identifikačních dokladů, pokud jsou zpracovávány, musí subjekt údajů dokázat předložením příslušných dokladů. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných OÚ, a to i poskytnutím dodatečného prohlášení.

Článek 12
PRÁVO SUBJEKTU NA VÝMAZ („PRÁVO BÝT ZAPOMENUT“)

Subjekt údajů má právo na to, aby Správce bez zbytečného odkladu vymazal OÚ, které se daného subjektu údajů týkají, a Správce má povinnost OÚ bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) OÚ již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování

c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, nebo subjekt údajů vznese námitky proti zpracování v případech zpracování pro účely přímého marketingu

d) OÚ byly zpracovány protiprávně

e) OÚ byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

Článek 13
OPRÁVNĚNÝ ZÁJEM SMCH

Subjekt údajů má právo na to, aby Správce omezil zpracování v kterémkoli z těchto případů:

a) subjekt údajů popírá přesnost OÚ, a to na dobu potřebnou k tomu, aby Správce mohl přesnost OÚ ověřit

b) zpracování je protiprávní a subjekt údajů odmítá výmaz OÚ a žádá místo toho o omezení jejich použití

c) Správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků

d) subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody Správce převažují nad oprávněnými důvody subjektu údajů.

Článek 14
PRÁVO NA PODÁNÍ NÁMITKY

Subjekt údajů má právo kdykoliv vznést námitku proti zpracování osobních údajů.

Článek 15
PRÁVO NA PŘENOSITELNOST ÚDAJŮ

1) Subjekt údajů má právo získat OÚ, které se ho týkají, jež poskytl Správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a právo předat tyto údaje jinému Správci, a to v případě že:

   a) zpracování je založeno na souhlasu se zpracováním osobních údajů (čl. 6 odst. 1 písm. a) Obecného nařízení) nebo na souhlasu se zpracováním zvláštní kategorie osobních údajů (čl. 9 odst. 2 písm. a) Obecného nařízení) nebo na smlouvě (čl. 6 odst. 1 písm. b) Obecného nařízení)

   b) zpracování se provádí automatizovaně.

2) Subjekt údajů má právo na to, aby OÚ byly předány přímo jedním Správcem Správci druhému, je-li to technicky proveditelné.

3) Tímto právem nesmí být nepříznivě dotčena práva a svobody jiných osob.

Článek 16
OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OÚ

1) Jakékoli porušení zabezpečení OÚ Správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

2) Ohlášení dozorovému úřadu musí obsahovat:

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

   b) kontaktní místo, které může poskytnout bližší informace

   c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů

   d) popis opatření, která Správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

3) Správce dokumentuje veškeré případy porušení zabezpečení OÚ, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Veškeré záznamy a dostupné informace o porušení ochrany osobních údajů budou uloženy v kanceláři Pověřence a na vyžádání budou přístupné dozorovému úřadu.

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

5) Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

   a) Správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u OÚ dotčených porušením zabezpečení OÚ, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup, jako je např. šifrování

   b) Správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů se již pravděpodobně neprojeví

   c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

6) Správce vede rovněž dokumentaci o potenciálních bezpečnostních incidentech, obsahující záznamy o skutečnostech, které by mohly způsobit porušení zabezpečení OÚ, přestože k porušení nedošlo nebo se v dané době neprojevilo. Tato dokumentace bude rovněž uložena v kanceláři Pověřence.

KAPITOLA 5
APLIKACE PODMÍNEK PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SMCH

Článek 1
ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V RÁMCI SMCH

1) V rámci SMCH je povoleno zpracovávat osobní údaje pouze za podmínek stanovených nařízením, zákony a touto směrnicí.
2) V rámci lidských zdrojů je možné zpracovávat osobní údaje o zaměstnancích stanovené zvláštními zákony (např. zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů, zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů, apod.), a to pro účely pracovněprávního vztahu a pro plnění úkolů uložených zákonem č. 262/2006 Sb., zákoníkem práce, ve znění pozdějších předpisů, nebo zvláštním právním předpisem, po dobu nezbytnou k zajištění práv a povinností, plynoucích z tohoto pracovněprávního nebo jiného obdobného vztahu.
3) SMCH jako orgán veřejné správy zpracovává převážnou většinu osobních údajů ze zákona. SMCH dále zpracovává osobní údaje ze smluv, na základě oprávněného zájmu nebo výjimečně se souhlasem subjektu údajů.

Článek 2
POVINNOSTI PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Pro zpracování OÚ platí následující povinnosti a pravidla:

a) všichni zaměstnanci jsou povinni zachovávat mlčenlivost o veškerých informacích, se kterými byli obeznámeni v souvislosti se zpracováním OÚ; povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo příslušných prací; mlčenlivost se vztahuje i na opatření, která slouží k zabezpečení zpracování OÚ

b) zaměstnanci nesmí umožnit nahlížet do OÚ či předávat OÚ neoprávněným osobám

c) zaměstnancům je zakázáno bezdůvodně pořizovat kopie nebo videozáznamy (fotografie) OÚ, ani pořizovat kopie souborů obsahující OÚ

d) u kopie dokumentu obsahující OÚ je potřeba uplatňovat stejná pravidla pro ochranu OÚ jako u originálu

e) zaměstnanci, kteří si pořídili kopii dokumentu obsahující OÚ výhradně pro pracovní potřebu, tuto kopii po skončení důvodu pro zpracování skartují či v případě elektronické kopie odstraní

f) všem zaměstnancům je zakázáno OÚ ukládat na soukromých paměťových médiích, soukromých počítačích a soukromých mobilních zařízeních

g) pokud bude k přenosu či předání dokumentů obsahujících OÚ třeba použít přenosné úložiště (flash disk, externí disk a další), bude toto přenosné úložiště zašifrováno takovým způsobem, aby se k osobním údajům nedostala neoprávněná osoba; adekvátní zajištění úložiště OÚ (např. šifrování), zajistí OIT a ohlásí k zaevidování tajemníkovi MMCH do seznamu úložišť

h) všem zaměstnancům je zakázáno zpracovávat OÚ na neschválených IT prostředcích

i) je zakázáno posílat dokumenty obsahující OÚ e-mailem mimo interní síť SMCH; v případě potřeby předání OÚ mimo interní síť SMCH, musí být přenos přiměřeně zajištěn, např. šifrováním dokumentu, anebo použitím zabezpečeného kanálu (v případě záměru použití zabezpečeného kanálu bude přizván OIT)

j) Všichni garanti agend, na jejichž odboru dochází ke zpracování osobních údajů, jsou povinni přijmout takové opatření (v případě technických opatření ve spolupráci s příslušnými organizačními jednotkami), aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k OÚ, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití. Tato povinnost platí i po ukončení zpracování OÚ.

Článek 3
EVIDENCE PŘIJATÝCH TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ

Podčlánek 3.1
PERSONÁLNÍ BEZPEČNOST

S osobními údaji se může seznámit pouze oprávněná osoba, a to v rozsahu odpovídajícím jejímu oprávnění. Oprávnění této osoby vyplývá z její pracovní náplně na základě uzavřeného pracovněprávního vztahu nebo obdobného vztahu. Oprávněná osoba musí mít objektivní a důvodnou potřebu seznámit se s osobními údaji za účelem plnění pracovních povinností či jiných povinností nebo oprávněných zájmů.

Podčlánek 3.2
FYZICKÁ BEZPEČNOST

1) Dokumenty s osobními údaji se ukládají na příslušných pracovištích (kanceláře, archivy apod.) v souladu se Spisovým řádem a ostatními interními předpisy.

2) Dokumenty obsahující osobní údaje musí být ukládány v uzamčených schránkách (kancelářské skříně, trezorové skříně, plechové skříně, stolní kontejnery apod.), bez možnosti přístupu neoprávněných osob v mimopracovní době i v době krátkodobé nepřítomnosti oprávněné osoby (oběd, přestávka apod.).

3) Klíči od uzamčené schránky disponuje určená osoba; duplikáty klíčů od kanceláří jsou uloženy u osoby pověřené Správcem ke zpracování OÚ v uzamykatelných skříních.

4) v době nepřítomnosti osoby pověřené Správcem ke zpracování OÚ může uzamčenou skříň s náhradními klíči od kanceláře bez souhlasu osoby pověřené Správcem ke zpracování OÚ otevřít

pouze nejblíže nadřízený zaměstnanec osoby pověřené Správcem ke zpracování OÚ nebo jím určená osoba.

5) Při skončení pracovněprávního vztahu osoby pověřené Správcem ke zpracování OÚ zabezpečí předání údajů jiné osobě nejblíže nadřízený zaměstnanec osoby pověřené Správcem ke zpracování OÚ; pokud není přebírající znám, osoba pověřená Správcem ke zpracování OÚ předá dokumenty nejblíže nadřízenému zaměstnanci, nebo dokumenty uloží do spisovny v zabezpečeném obalu, ke kterému přiloží seznam ukládaných dokumentů.

Podčlánek 3.3
INFORMAČNÍ BEZPEČNOST OSOBNÍCH ÚDAJŮ UKLÁDANÝCH V ICT SMCH

Zabezpečení přístupu k osobním údajům zpracovávaných v ICT SMCH vychází ze směrnic č.:

- 2023 - 16 pro správu a užívání informačních a komunikačních technologií MMCH
- 2023 - 17 k realizaci bezpečností politiky ISVS MMCH
- 2023 - 18 pro činnost bezpečnostního správce ISVS MMCH
- 2023 - 19 Systémová příručka inf. bezpečnosti IS MMCH

Článek 4
NOVÉ ZPRACOVÁNÍ OÚ, ZMĚNA STÁVAJÍCÍHO ZPRACOVÁNÍ OÚ

1) Nové zpracování, či změnu stávajícího zpracování OÚ zajišťuje odpovědný garant agendy při současném zohlednění zásad zpracování OÚ dle kapitoly 4, článku 1 této směrnice.
2) V případě nového zpracování či změny stávajícího zpracování OÚ je příslušný garant agendy povinen vypracovat, či aktualizovat příslušný záznam o činnostech zpracování OÚ (v případě technických opatření ve spolupráci s příslušnými odbory – OIT, či úseky - Provoz aj.), a odeslat jej k vyjádření Pověřenci.
3) Na základě nového, či aktualizovaného Datového inventurního záznamu provede tajemník MMCH vyhodnocení nutnosti DPIA a v případě potřeby zajistí jeho realizaci.
4) Pověřenec zajistí ve spolupráci s garantem agendy, OIT a Provozem analýzu rizik (případně aktualizaci) dopadu konkrétního zpracování na subjekty osobních údajů.

Článek 5
LIKVIDACE OSOBNÍCH ÚDAJŮ

1) Po ukončení zpracování OÚ, nebo na základě oprávněné žádosti subjektu OÚ zajistí likvidaci OÚ příslušný garant agendy.
2) Při likvidaci těchto údajů je nutné vyplnit Likvidační protokol (viz Příloha č. 7), který musí být podepsán 2 oprávněnými zaměstnanci, které určí příslušný garant agendy. Protokoly o likvidaci OÚ eviduje odpovědný garant agendy nebo jím pověřený pracovník.

3) Dokumenty musí být likvidovány v souladu s interním předpisem Spisový a skartační řád.

4) Likvidaci fyzických dokumentů zajišťuje příslušný pracovník (oprávněný pracovník za účasti druhého oprávněného pracovníka) skartováním.

5) Vymazání OÚ z úložišť a systémů zajišťuje OIT.

Článek 6
EVIDENCE ÚLOŽIŠŤ OÚ

1) Evidenci úložišť na jednotlivých odborech či organizačních složkách vede Garant agendy. Evidenci všech úložišť OÚ v SMCH vede tajemník MMCH.

2) Zabezpečení datových úložišť OÚ, např. centrální datové úložiště a informační systémy nebo pevný disk osobního počítače zajišťuje OIT.

3) Zabezpečení přenosných úložišť OÚ, např. přenosná úložiště (flash disk, externí pevný disk) nebo úložiště přenosných zařízení (notebook, mobilní telefon, tablet) zajišťuje příslušný zaměstnanec, kterému byly přiděleny v součinnosti s OIT.

4) Zabezpečení fyzických úložišť OÚ, např. úložiště fyzických dokumentů zajišťuje Provoz.

5) V případě změny nebo aktualizace zabezpečení úložišť zašle OIT nebo Provoz požadavek na změnu, resp. aktualizaci k vyjádření tajemníkovi MMCH a k provedení aktualizace Evidence úložišť.

6) Tajemník MMCH následně ve spolupráci s příslušným garantem agendy provede aktualizaci Datových inventurních záznamů.

Článek 7
POSTUPY SPRÁVCE PŘI VÝKONU PRÁV SUBJETKŮ ÚDAJŮ

1) Subjekt údajů je oprávněn žádat o:

   a) přístup k OÚ
   b) opravu OÚ
   c) výmaz OÚ
   d) omezení zpracování, vznést námitku.

2) Subjekt údajů za účelem výkonu svých práv může po ověření totožnosti podat žádost osobně, písemně s úředně ověřeným podpisem či v elektronické formě (prostřednictvím datové schránky, emailem s elektronickým podpisem opatřeným kvalifikovaným certifikátem).

3) SMCH předá informaci či jinak vyřídí žádost subjektu údajů ve formě preferované subjektem údajů. Pokud ji subjekt údajů nezvolil, platí, že odpověď a další komunikace probíhá ve formě odpovídající podané žádosti. V případě, že subjekt údajů podal žádost v elektronické formě, SMCH poskytne informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.

4) Po převzetí žádosti buď Pověřencem v kanceláři Pověřence nebo na podatelně MMCH, která žádost neprodleně předá Pověřenci, bude Pověřencem žádost zaevidována, následně bude o žádosti informován tajemník MMCH a bude zahájeno její vyřízení.

5) Evidence žádostí bude vedena v elektronické podobě na sdílené složce na centrálním datovém úložišti, kam budou mít přístup pouze Pověřenec a tajemník MMCH.

6) SMCH je povinno podle náležitostí přijaté žádosti bez zbytečného odkladu, a vždy do jednoho měsíce od obdržení žádosti, poskytnout žadateli informace o přijatých krocích. Lhůtu jednoho měsíce je možné o další dva měsíce prodloužit s ohledem na složitost a počet žádostí přijatých během období jednoho měsíce od přijetí žádosti. V prodloužené lhůtě nelze žádost odmítnout. SMCH musí informovat žadatele o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

7) Odpověď na žádost ve stanovené lhůtě zajistí odbor kanceláře tajemníka.

8) Pokud SMCH žádost odmítne, bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti informuje žadatele o důvodech odmítnutí a o možnosti podat stížnost u Dozorového úřadu a žádat o soudní ochranu.

9) SMCH poskytuje informace v rámci výkonu práv subjektu údajů bezplatně.

10) V případě, že SMCH žádost vyhodnotí jako zjevně nedůvodnou nebo nepřiměřenou, má právo žádost odmítnout nebo vyřízení žádosti zpoplatnit. SMCH před vyměřením přiměřeného poplatku žadatele o jeho výši informuje a zjistí, zdali žadatel i přes vyměřený poplatek požaduje poskytnutí informací. Po zaplacení poplatku budou žadateli informace předány ve lhůtě do jednoho měsíce od zaplacení poplatku.

11) SMCH je povinno oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy, likvidaci osobních údajů nebo omezení zpracování s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí.

12) Tajemník MMCH společně s Pověřencem a s pomocí OIT, případně s příslušným garantem agendy:

    a) v případě žádosti o přístup k OÚ:

        - zajistí informaci, zda jsou o dotyčném subjektu zpracovávány OÚ
        - informuje subjekt o zpracovávaných údajích v rozsahu Záznamu o zpracování
        - pokud to subjekt požaduje, poskytne buď fyzickou, nebo elektronickou kopii zpracovávaných OÚ

    b) v případě žádosti o opravu:

        - ověří a zajistí aktualizaci příslušných OÚ v souladu s požadavkem subjektu,
        - informuje subjekt o provedení aktualizace osobních údajů.

    c) v případě žádosti o výmaz:

        - rozhodne, zda je žádost o výmaz oprávněná a pokud ano, zajistí výmaz předmětných OÚ,
        - informuje subjekt o výmazu příslušných OÚ, případně o nemožnosti výmaz provést, a to včetně odůvodnění nemožnosti.

d) v případě vznesení námitky či žádosti o omezení zpracování:

- rozhodne, zda je žádost na omezení zpracování oprávněná a pokud ano, zajistí pozastavení zpracování předmětných OÚ. Pokud není oprávněná, informuje o této skutečnosti neprodleně subjekt údajů,
- informuje subjekt o pozastavení či následné obnově pozastaveného zpracování.

e) v případě požadavku na přenositelnost OÚ:

- rozhodne, zda je žádost o přenositelnost OÚ oprávněná a pokud ano, zajistí předání OÚ ve strukturovaném, běžně používaném a strojově čitelném formátu
- zajistí předání OÚ ve strukturovaném, běžně používaném a strojově čitelném formátu subjektu údajů nebo přímo novému Správci, je-li to technicky proveditelné.

13) V případě obnovy dat ze záloh zajistí OIT na základě Evidence požadavků subjektu OÚ prověření a opětovné smazání příslušných OÚ dříve, než budou systému uvolněny zpět do produkčního provozu.

Článek 8
HLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OÚ

1) Zaměstnanec, který zjistí porušení zabezpečení osobních údajů, nahlásí tuto skutečnost neprodleně tajemníkovi MMCH a Pověřenci pro ochranu osobních údajů.

2) Tajemník MMCH ve spolupráci s pověřencem informuje příslušného garanta agendy o porušení zabezpečení OÚ.

3) Pověřenec vyhodnotí pravděpodobnost rizika porušení zabezpečení pro práva a svobody fyzických osob a v souladu s ustanoveními článku 14 GDPR riziko porušení zabezpečení ohlásí dozorovému úřadu. V případě vysokého rizika pro práva a svobody fyzických osob ohlásí riziko porušení zabezpečení i subjektu údajů.

4) Pověřenec dokumentuje veškeré případy porušení zabezpečení osobních údajů v Evidenci porušení zabezpečení OÚ, přičemž uvede skutečnosti, které se týkají daného porušení, jeho dopady a přijatá nápravná opatření. Tato dokumentace musí být na vyžádání přístupná dozorovému úřadu.

5) Garant agendy odpovědný za zpracování příslušných OÚ zajistí ve spolupráci s pověřencem, tajemníkem MMCH, a příslušnými organizačními jednotkami nápravná opatření a provede případné změny v Datovém inventurním záznamu.

Článek 9
HLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OÚ DOZOROVÉMU ORGÁNU

1) Tajemník MMCH ve spolupráci s Pověřencem a dotčenými útvary zahájí interní vyšetřování. Pokud ze závěru interního vyšetřování vyplývá, že k porušení zabezpečení osobních údajů došlo a je zde riziko pro práva a povinnosti fyzických osob, ohlásí Pověřenec tuto skutečnost bez zbytečného odkladu Úřadu.

2) Ohlášení musí být doručeno Úřadu bez zbytečného odkladu, nejpozději do 72 hodin od zjištění skutečnosti, která s vysokou pravděpodobností představuje porušení zabezpečení osobních údajů. Pokud do této lhůty není ohlášení Úřadu doručeno, musí být zároveň s ohlášením uvedeny relevantní důvody tohoto zpoždění.

3) Ohlášení musí mít písemnou formu a musí obsahovat:

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

   b) jméno a kontaktní údaje Pověřence

   c) popis pravděpodobných důsledků, které porušení zabezpečení osobních údajů představuje

   d) popis nápravných opatření, která byla přijata nebo navržena k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů

   e) organizace oznámí bez zbytečného odkladu po ukončení interního vyšetřování porušení zabezpečení osobních údajů, pokud toto porušení bylo v závěru interního vyšetřování vyhodnoceno jako vysoce rizikové pro práva a povinnosti fyzických osob.

4) Oznámení není nutné činit v případě, že:

   a) byla zavedena náležitá technická a organizační opatření a tato 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 (např. šifrování)

   b) byla přijata nápravná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví

   c) podání oznámení vyžaduje nepřiměřené úsilí. V takovém případě musí být subjekt údajů informován stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Článek 10
UZAVŘENÍ SMLOUVY SE ZPRACOVATELEM OÚ

Přípravu smlouvy se Zpracovatelem OÚ zajišťuje příslušný garant agendy ve spolupráci s právním úsekem odboru interního auditu. Smlouva musí respektovat ustanovení kapitoly 4, článku 9 této směrnice.

Článek 11
POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

1) SMCH stanoví, kdo a jakým způsobem zajišťuje roli Pověřence.

2) Pověřenec je zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů v SMCH.

3) Pověřenec není odpovědný za nedodržení pravidel stanovených nařízením a touto směrnicí při postupech v oblasti osobních údajů.

4) Je zakázáno uložit pověřenci pokyny týkající se výkonu jeho úkolů.

5) Pověřenec je vázán povinností mlčenlivosti ohledně skutečností, které se dozvěděl při výkonu své funkce, a to i po skončení smluvního či pracovněprávního vztahu.

6) Vedení SMCH oznámí vhodným způsobem Úřadu, veřejnosti a všem zaměstnancům kontaktní údaje Pověřence.

7) Subjekty údajů se mohou obracet na Pověřence ve všech záležitostech souvisejících se zpracováním osobních údajů a výkonem jejich práv. Žádosti a stížnosti subjektů údajů budou vyřízeny dle této směrnice.

8) Pověřenec nesmí při své činnosti určovat účely nebo prostředky zpracování osobních údajů.

9) Pověřenec se nesmí dostat do situace, kdy by sám kontroloval své vlastní postupy.

Článek 12
VZDĚLÁVÁNÍ

Tajemník MMCH zajistí pravidelné vzdělávání zaměstnanců, kteří přichází do styku s osobními údaji.

Článek13
ODPOVĚDNOST A POVINNOST SPRÁVCE PŘI ZPRACOVÁNÍ OÚ

1) SMCH jako Správce odpovídá za dodržování jednotlivých povinností stanovených právními předpisy, upravujícími ochranu osobních údajů.

2) SMCH má definované role a odpovědnosti při zpracování osobních údajů v rámci své působnosti (ustanovené organizačním/pracovním řádem a pracovními náplněmi).

3) SMCH vystupuje převážně v roli Správce.

4) Zmocnění ke zpracování osobních údajů vyplývá ze zvláštního právního předpisu nebo ze smlouvy o zpracování osobních údajů, případně z uděleného Souhlasu od subjektu. Ve všech případech musí být dostatečným způsobem upraveny požadavky na vhodná technická a organizační opatření na ochranu osobních údajů.

5) Pokud se na zpracování osobních údajů v gesci Správce podílí třetí strana (Zpracovatel), pak smí SMCH využít pouze takového Zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky stanovené nařízením a touto směrnicí a aby byla zajištěna ochrana práv subjektů. Smlouva o zpracování osobních údajů Zpracovatelem musí mít písemnou formu a splňovat veškeré podmínky kladené na takovouto smlouvu v kapitole 4, článku 9 této směrnice.

6) SMCH v pozici Správce určuje účely a prostředky zpracování osobních údajů a nese za tuto činnost odpovědnost. Jestliže SMCH zjistí, že Zpracovatel porušuje povinnosti stanovené nařízením, je

povinno na tuto skutečnost Zpracovatele neprodleně upozornit a ukončit zpracování osobních údajů Zpracovatelem.

7) SMCH jako Správce nebo Zpracovatel spolupracuje na požádání s Úřadem při plnění jeho úkolů.

KAPITOLA 6
KAMEROVÝ SYSTÉM

1) MMCH provozuje stacionární kamerový systém v celkovém počtu 30 stacionárních kamer a 1 serveru k ukládání záznamů kamer.

2) Záznamový server Hikhvision je umístěn v kanceláři OIT č. 101, Zborovská 4602, 430 28 Chomutov.

   Kamery připojené na tento záznamový server se nachází
   - 3 kamery v budově Radnice, nám. 1. Máje
   - 27 kamer v budově Magistrátu, Zborovská 4602..

3) Přesné rozmístění jednotlivých kamer je zakresleno v pláncích v příloze č. 8 této směrnice.

4) U vchodu do každé budovy MMCH jsou zaměstnanci, zastupitelé i návštěvníci upozorněni informativní tabulkou na skutečnost, že prostor do kterého vstupují, je monitorován kamerovým systémem se záznamem.

5) Účelem zpracování osobních údajů pořízených stacionárním kamerovým systémem je ochrana osob a majetku, konkrétně zajištění bezpečnosti zastupitelů, zaměstnanců magistrátu a osob z řad veřejnosti („návštěvníci MMCH“) pohybujících se v objektech magistrátu, ochrana osobnostních práv, zdraví a majetku zastupitelů, zaměstnanců a veřejnosti, jakož i majetku magistrátu. Sledovaného účelu nelze účinně dosáhnout jinou cestou.

6) Záznamy obrazových záběrů jsou pořizovány rovněž za účelem jejich možného využití k identifikaci fyzických osob oprávněnými státními orgány.

7) Stacionární kamerový systém běží nepřetržitě 24 hodin denně. Za jeho provozuschopnost odpovídá vedoucí Provozu.

8) Záznamy z kamer jsou ukládány na interní pevné disky záznamového serveru. Prostory umístění serverů jsou chráněny elektronickým zabezpečovacím systémem, aby byl zamezen přístup neoprávněných osob. Přístup do záznamového serveru je chráněn heslem.

9) V případě kamerovým systémem dokumentovaných porušení práv zastupitelů, zaměstnanců a veřejnosti, jakožto i škod na majetku statutárního města Chomutova, se zaznamenaná data (záznamy) zpřístupní (do doby jejich likvidace) příslušným orgánům (např. orgány činné v trestním řízení, soudy). Přístup k prohlížení záznamů zajišťují pracovníci IOT na základě příkazu tajemníka. Vydání záznamů zajišťují pracovníci OIT na základě příkazu tajemníka, který je vydán na základě žádosti o vydání věci oprávněnému orgánu.

10) Za zpracování osobních údajů pořízených stacionárním kamerovým systémem v souladu se zákonem odpovídá tajemník.

11) Záznamy pořízené kamerami se uchovávají po dobu 48 hodin, poté jsou vymazány neobnovitelným způsobem. Lhůta 48 hodin se počítá od následujícího dne po jejich pořízení.

12) Po uplynutí této lhůty jsou uložené záznamy automaticky přepsány a tím nevratně a trvale vyloučeny z dalšího zpracování.

KAPITOLA 7
ZÁVĚREČNÁ USTANOVENÍ

1) Všichni zaměstnanci jsou povinni se prokazatelně (proti podpisu) seznámit s touto směrnicí.
2) Odborný výklad k této směrnici podá Pověřenec.

SEZNAM PŘÍLOH

Příloha č. 1 – Datové inventurní záznamy

Příloha č. 2 – Záznam o činnostech zpracování

Příloha č. 3 – Evidence požadavků subjektu údajů

Příloha č. 4 – Evidence porušení zabezpečení OÚ

Příloha č. 5 - Evidence potenciálních bezpečnostních incidentů

Příloha č. 6 - Evidence souhlasů

Příloha č. 7 - Likvidační protokol

Příloha č. 8 - Rozmístění kamer a informační cedule

Údaj	Účel zpracování	Právní titul
Jméno, příjmení	Výběr vhodného žadatele o zaměstnání	Zpracování je nezbytné pro splnění (resp. uzavření) smlouvy
	Uzavření pracovní smlouvy	Zpracování je nezbytné pro splnění či uzavření smlouvy
	Evidence pracovní doby, plnění právních a smluvních povinností	Zpracování je nezbytné pro splnění právní povinnosti (§ 96 ZP)
	Evidence docházky pro potřeby kontroly plnění povinností ze strany zaměstnavatele - kontrola dodržování povinností zaměstnanců	Oprávněné zájmy správce? Plnění smlouvy?

ZÁZNAM O ČINNOSTECH ZPRACOVÁNÍ

Statutární město Chomutov jako Správce osobních údajů

Odbor	
Pořadové číslo záznamového listu	
Účel zpracování + popis operace	
Způsob zpracování	
Subjekt údajů	
Zpracovávané osobní údaje	
Právní titul zpracování	
Zpracovávané citlivé osobní údaje	

Právní titul zpracování citlivých osobních údajů	
Zdroj osobních údajů	
Příjemce osobních údajů	
Předávání osobních údajů do třetí země	
Program/aplikace	
Jak a kde jsou osobní údaje uloženy	
Správce aplikace	
Doba uchování + likvidace osobních údajů	

EVIDENCE POŽADAVKŮ SUBJEKTU ÚDAJŮ

Subjekt údajů: …….

Dne ……..

požádal o:

- ☐ přístup k informacím
- ☐ opravu osobních údajů
- ☐ výmaz osobních údajů
- ☐ omezení zpracování
- ☐ předání OÚ, které správci poskytl ve strojově čitelném formátu jinému správci

případně

- ☐ vznesl námitku

Žádost subjektu údajů byla vypořádána následovně:

…….

…….

…….

…….

(popis procesu, např.:

- byly mu předány informace o zpracování jeho OÚ, byl vyzván k úhradě přiměřeného poplatku, žádost byla zamítnuta nebo o něm nezpracováváme žádné OÚ.
- osobní údaje byly opraveny (a byl o tom vyrozuměn i příjemce/nebyl, protože je to moc náročné)
- osobní údaje byly vymazány, osobní údaje nebyly vymazány (správce OÚ potřebuje)
- zpracování bylo omezeno, nebylo omezeno

- údaje byly předány jinému správci, nebyly předány
- na základě podané námitky správce dále OÚ nezpracovává, správce dále zpracovává, protože prokázal, že jeho závažné oprávněné zájmy převyšují nad zájmy nebo právy a svobodami subjektu údajů)

V Chomutově, dne: ……

Pověřenec: ……

EVIDENCE PORUŠENÍ ZABEZPEČENÍ OÚ

Dne ……. v čase od …… do …… došlo k porušení zabezpečení osobních údajů.

K porušení zabezpečení osobních údajů došlo:

……

……

……

……

(popis situace)

Toto porušení mělo za následek:

……

……

……

……

(Popis buď již nastalých nebo pravděpodobných negativních následků pro subjekty údajů; šlo o nízké, střední nebo vysoké riziko pro práva a svobody fyzických osob?)

Jaká byla přijata nápravná opatření:

……

……

……

……

(aby se neopakovalo)

Porušení zabezpečení bylo oznámeno Úřadu pro ochranu osobních údajů dne…….

Bylo porušení zabezpečení s ohledem na riziko pro subjekty údajů oznámeno subjektům údajů:

- ☐ Ano, porušení mělo za následek vysoké riziko pro práva a svobody fyzických osob
- ☐ Ne, porušení nemělo za následek vysoké riziko pro práva a svobody fyzických osob
- ☐ Ne, správce zavedl náležitá technická a organizační ochranná opatření způsobující nesrozumitelnost údajů pro neoprávněné osoby, správce přijal následná opatření, která způsobí, že se vysoké riziko pravděpodobně neprojeví nebo by takovéto oznámení vyžadovalo nepřiměřené úsilí.

V Chomutově, dne……

Pověřenec: ……

EVIDENCE POTENCIÁLNÍCH BEZPEČNOSTNÍCH INCIDENTŮ

Dne …… došlo ve statutárním městě Chomutov k incidentu, jenž mohl potenciálně přerůst v porušení zabezpečení osobních údajů (potenciální bezpečnostní incident). K porušení zabezpečení osobních údajů však nedošlo nebo porušení zabezpečení osobních údajů nevyšlo nikterak najevo.

Potenciální bezpečnostní incident spočívá v tom, že:

……

……

……

……

(popis incidentu)

Proč zůstalo pouze u potenciálního bezpečnostního incidentu a nedošlo k porušení zabezpeční OÚ:

……

……

……

……

(pokud možno, tak popsat, proč nedošlo k ničemu závažnému)

Přijatá opatření:

……

……

……

……

V Chomutově, dne ……

Pověřenec:……..

EVIDENCE SOUHLASU

Souhlas č. …….

Jméno subjektu údajů: ……

Datum udělení souhlasu subjektem údajů: ……

Souhlas byl udělen za účelem: ……

Subjekt údajů byl před udělením souhlasu seznámem s:

- tím, kdo je Správcem osobních údajů a Pověřencem pro ochranu osobních údajů
- účelem zpracování
- tím, jestli budou jeho sobní údaje předávány dalším Správcům nebo zpracovatelům či nikoliv
- dobou zpracování osobních údajů
- právy subjektu údajů - právo na přístup k OÚ, právo na výmaz nebo opravu, omezení zpracování, právo vznést námitku proti zpracování a právo na přenositelnost údajů
- tím, že souhlas může kdykoliv odvolat (tím však nebude dotčena zákonnost předchozího zpracování založeného na souhlasu před odebráním souhlasu)
- tím, že má právo podat stížnost u dozorového úřadu

Souhlas byl udělen v písemné formě.

Za odbor ……, vedoucí odboru ……..

Tento souhlas byl odvolán dne …….

Za odbor ……, vedoucí odboru ……..

LIKVIDAČNÍ PROTOKOL

1. Útvar likvidující osobní údaje: ……

2. Název materiálu obsahujícího osobní údaje (pokud se jedná o více subjektů údajů, uvést výčet v příloze k protokolu):

……

……

……

……

3. Způsob likvidace:

……

……

……

4. Místo likvidace:

……

……

5. Datum likvidace (popř. údaj o době, po které je likvidace prováděna):

……

6. Jméno a podpis vedoucího, který schválil likvidaci:

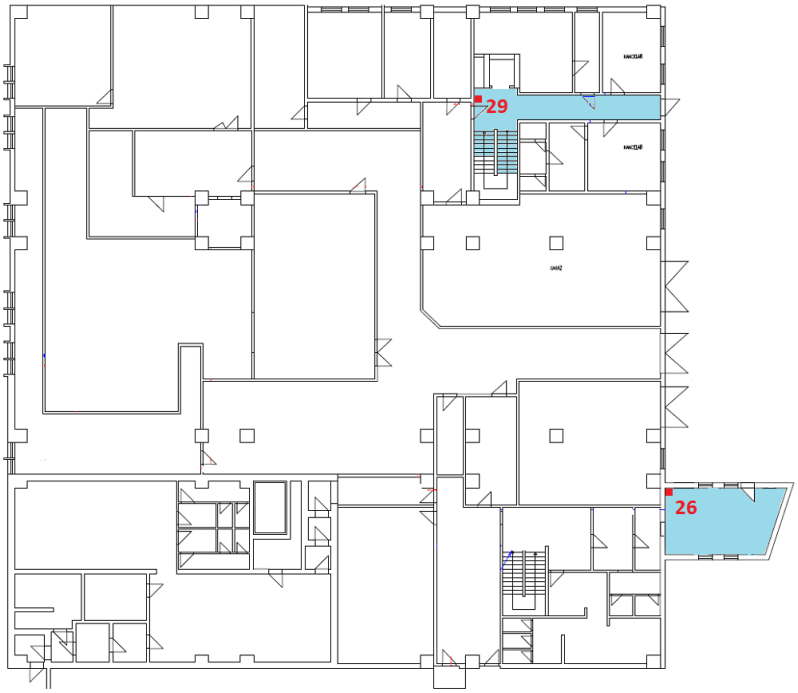
…… .....

7. Jméno a podpisy dvou zaměstnanců určených vedoucím útvaru, kteří odpovídají za provedení likvidace:

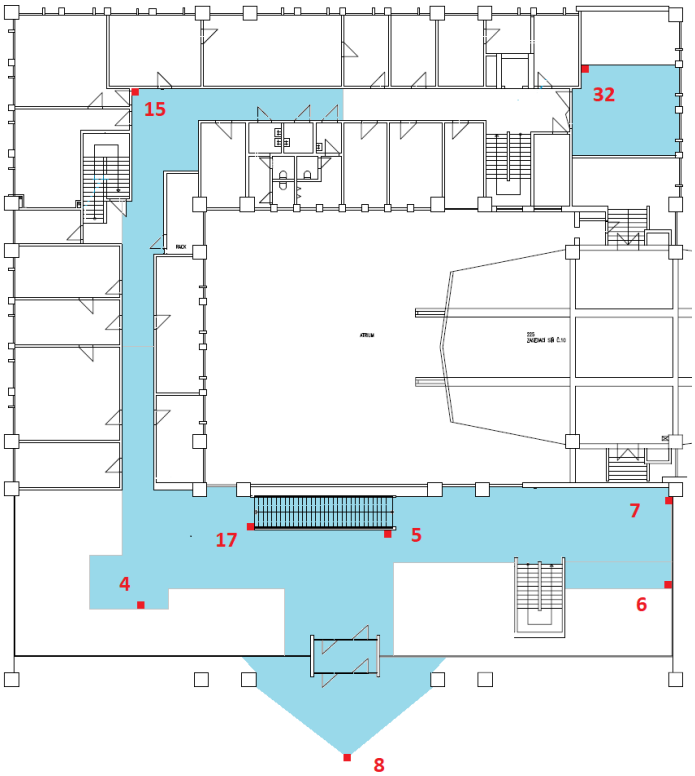
…… ……

Příloha č. 8 – Rozmístění kamer

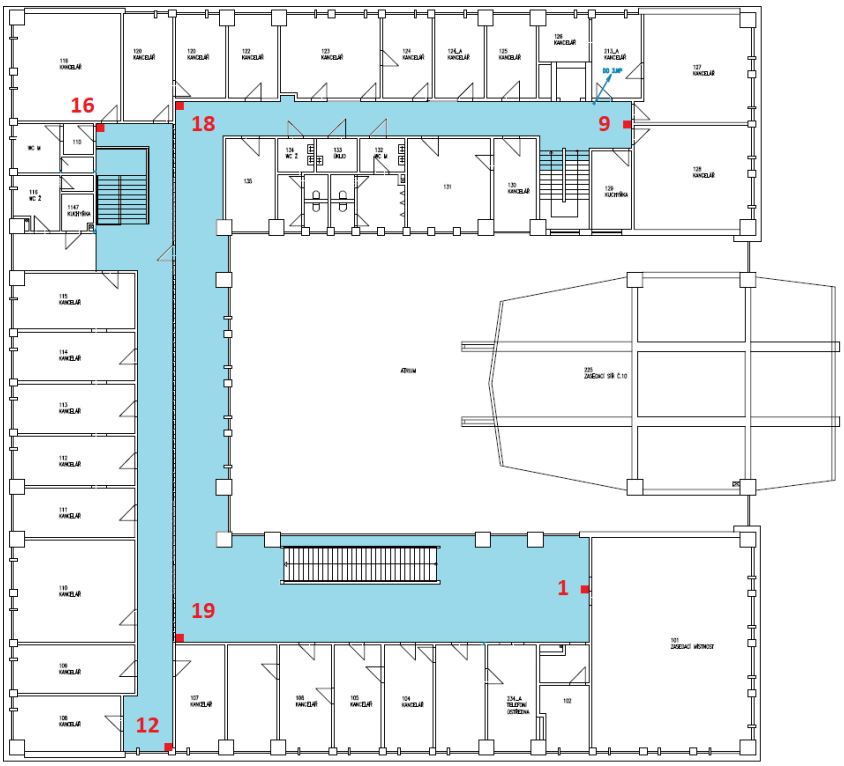
1.PP - MMCH Zborovská



1.NP - MMCH Zborovská

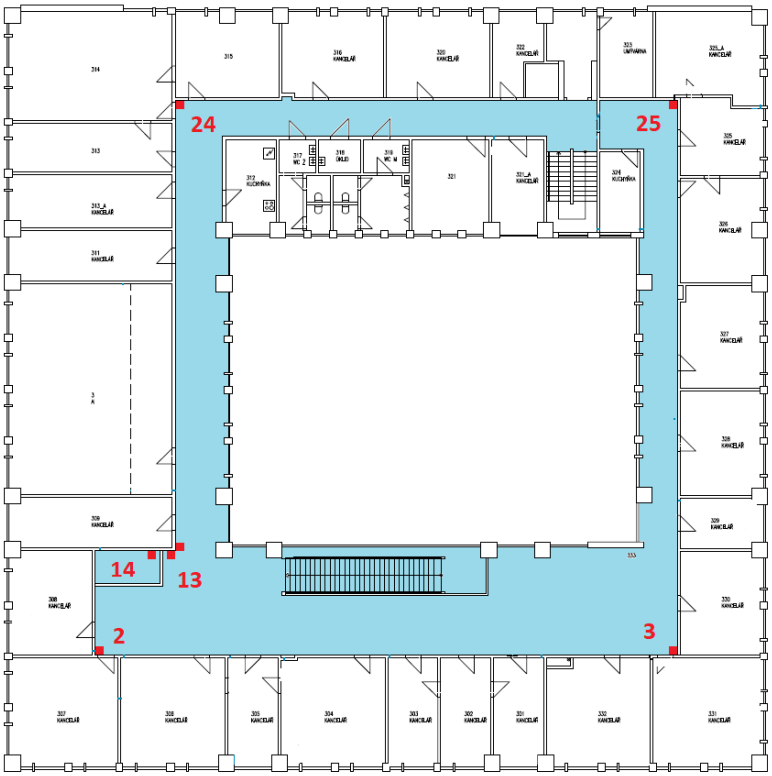


2.NP - MMCH Zborovská

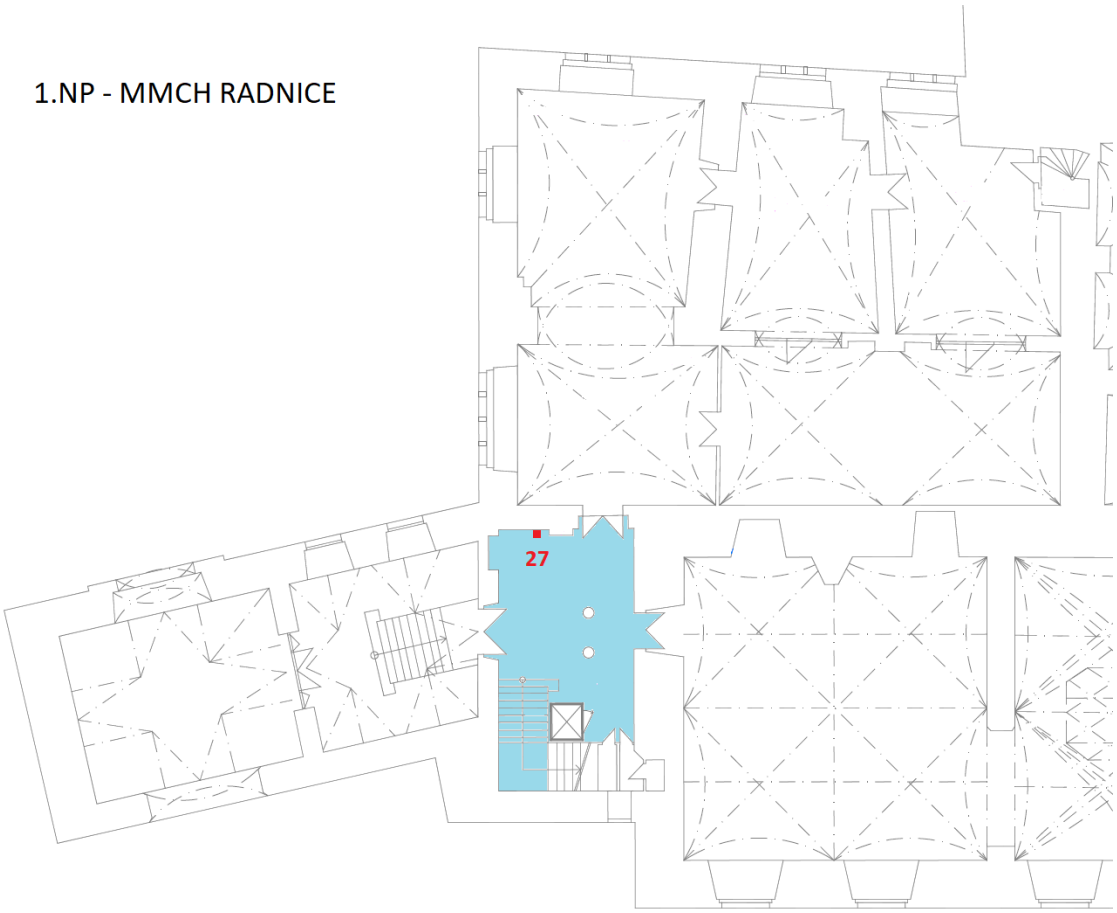


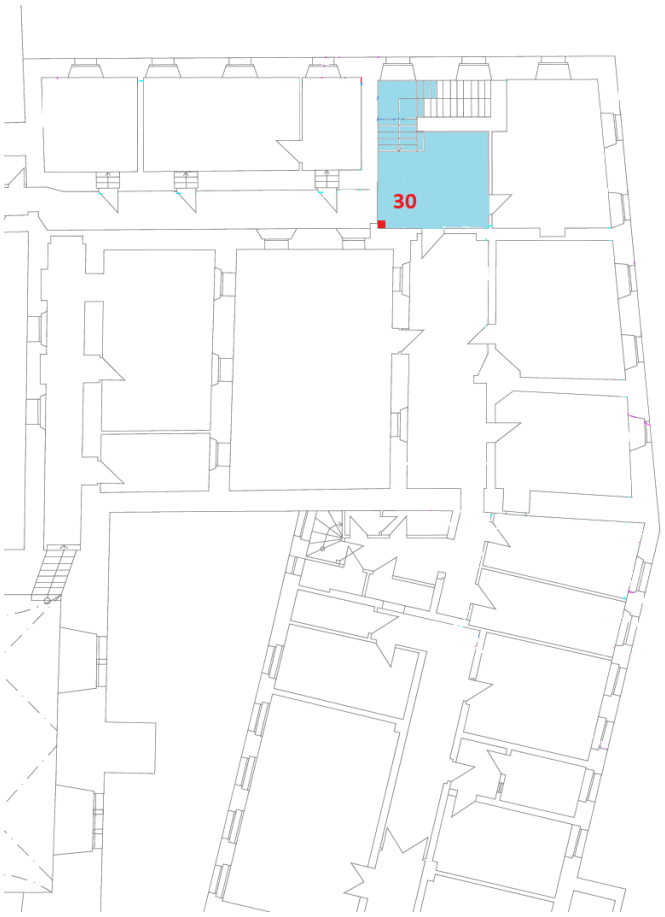
3.NP - MMCH Zborovská

4.NP - MMCH Zborovská



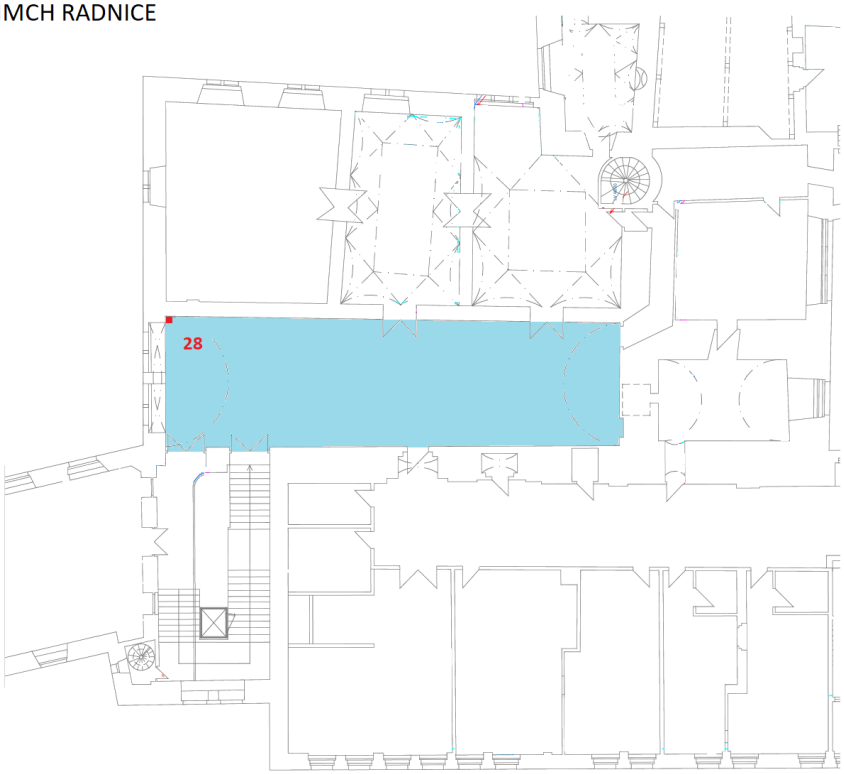
1.NP - MMCH RADNICE





1.NP - MMCH RADNICE

2.NP - MMCH RADNICE



Informační cedule