ÚŘAD PRÁCE ČESKÉ REPUBLIKY
KRAJSKÁ POBOČKA V PLZNI

Druh interního aktu: **Směrnice ředitele krajské pobočky č. 2/2016**	**Č.j. UPCR-PM-2016/2180-00832210**
Název aktu: **K zabezpečení ochrany osobních údajů**	
Zrušuje: Směrnici ředitele KrP č. 6/2012 ve znění dodatků č. 1 a 2	
Účinnost od: 15.1.2016	*Účinnost do:* **na dobu neurčitou**

Za navrhovatele: JUDr. Rudolf Tomášek, ředitel kanceláře krajské pobočky Mgr. Michal Kadlec, ředitel odboru kontrolně právního	*Datum:* 14.1.2016 14.1.2016	*Podpis:* JUDr. Tomášek, v.r. Mgr. Kadlec, v.r.
Kontroloval z hlediska formálně právního: Mgr. Michal Kadlec, ředitel odboru kontrolně právního krajské pobočky	*Datum:* 14.1.2016	*Podpis:* Mgr. Kadlec, v.r.
Schválil: Ing. Zdeněk Novotný, ředitel krajské pobočky	*Datum:* 14.1.2016	*Podpis:* Ing. Novotný, v.r.

Počet originál. výtisků:	*Číslo výtisku:*	*Skartační režim:*
1	1	**A** výtisk č. 1, **S 1** ostatní

K provedení Směrnice GŘ č. 10/2012 „Směrnice k zajištění ochrany osobních údajů“ (Směrnice GŘ) vydávám tuto Směrnici ÚP ČR – krajské pobočky v Plzni (dále také jen „krajská pobočka“ nebo „KrP“):

Článek I
Ochrana osobních údajů

1. Technicko-organizační zabezpečení ochrany osobních údajů je prováděno prostřednictvím režimových opatření pro budovy, ve kterých úřad práce působí a režimových opatření pro klíče a přístupové resp. docházkové karty. Režimy přístupů do budov, zajištění ostrahy a ochrany budov, klíčové a kartové režimy jsou uvedeny ve Směrnici krajské pobočky „Provozní řády budov“. K režimu používání klíčů se ukládá všem zaměstnancům dbát v případě opuštění kanceláří, případně jiných místností, kde by mohlo dojít k přístupu k osobním údajům, na jejich řádné uzamykání.

2. Technicko-organizační zabezpečení ochrany osobních údajů je prováděno také prostřednictvím režimových opatření v oblasti čipových karet k přístupu do počítačů resp. informačních systémů a agendových aplikací. Pro tento režim zejména platí pravidla Provozního řádu informačních systémů MPSV, mimo jiné:
   a) Přístupový účet je standardně tvořen zejména certifikátem uloženým na čipové kartě zaměstnance a PIN kódem čipové karty[1]. Čipové karty vydává pro zaměstnance MPSV, a to na základě řádné podané žádosti. Při ukončení pracovněprávního nebo služebního vztahu zaměstnanec kartu prokazatelně vrací. Čipové karty (vydávání, vracení) spadají na KrP do působnosti oddělení informatiky.
   b) PIN kód k čipové kartě musí zaměstnanec zachovávat v tajnosti, zejména jej nesděluje jiným osobám nebo jej nepřevádí do písemné nebo elektronické podoby tak, že by mohl být přístupný třetím osobám.
   c) Přestane-li zaměstnanec na počítači vykonávat činnost, je povinen se od počítače odhlásit, nebo jinak počítač zajistit před neoprávněným přístupem. Vhodnou formou je stisknutí kombinace klávesy s logem Windows a klávesy L (případně stisknutí kombinace kláves Ctrl+Alt+Del a položky „Uzamknout tento počítač“). Povinnost má zaměstnanec i tehdy, opustí-li kancelář či místnost, ve které je počítač umístěn, přeruší-li svoji práci na dobu delší než 10 minut nebo tak hodlá učinit.
   d) Před neoprávněným přístupem je nutno chránit i nosiče informací (pevné disky, diskety, USB flash disky, pásková média, různé typy paměťových médií a další zařízení, na kterých lze přenášet a uchovávat data).

3. S osobními údaji mohou nakládat jen ti zaměstnanci, u kterých to věcně odpovídá jejich druhu práce a schválenému popisu pracovní činnosti.

4. Pracuje-li zaměstnanec s osobními údaji, nesmí je sdělovat ani ostatním zaměstnancům úřadu, kteří s nimi nejsou oprávněni pracovat a musí se chovat tak, aby se s nimi nemohla seznámit jiná třetí osoba (odezírání z monitoru počítače, ponechaný vytištěný papírový nosič a podobně).

5. V souladu s čl. 3 bodem 5 Směrnice GŘ jsou zaměstnanci povinni osobní údaje fyzicky dostupné ve formě žádosti o příspěvek či dávku prostřednictvím agendových aplikací uchovávat v uzamykatelných schránkách (skříních),

[1] Výjimečně může správce systému tj. MPSV přistoupit k jinému způsobu zabezpečení přístupu.

uzamykatelných místnostech a uzamykatelných budovách (viz také bod 1 této Směrnice).

6. Zaměstnanec, který má přístup nebo zpracovává osobní údaje (zejména pracující s datovými větami žádostí o příspěvek či dávku prostřednictvím agendových aplikací a s informačními systémy a databázemi agendových aplikací), je povinen o těchto údajích zachovávat mlčenlivost. Výjimkou je, pokud zvláštní zákon (trestní řád, občanský soudní řád, exekuční řád atd.) ukládá povinnost informaci poskytnout. Povinnost mlčenlivosti trvá i po skončení pracovního nebo služebního poměru. Mlčenlivosti může být zaměstnanec zbaven v souladu se zákonem (např. § 303 odst. 2 zákoníku práce, § 77 zákona o státní službě, § 147a zákona o zaměstnanosti, § 20 kontrolního řádu).

7. Porušení povinností zaměstnance vyplývající z výše uvedeného, může být dle klasifikováno jako porušování povinnosti zaměstnance vyplývající z právních předpisů vztahujících se k vykonávané práci s následky dle § 52 nebo § 55 zákoníku práce nebo zaviněné porušení služební kázně podle zákona o státní službě s následky vzniku kárné odpovědnosti, případně jako jiné porušení se sankcemi dle zvláštních právních předpisů (např. neoprávněné nakládání s osobními údaji - trestní zákon, porušení dle zákona o ochraně osobních údajů apod.).

Článek II
Klasifikace informací

1. Každý zaměstnanec je povinen nově vytvářenou informaci (jako její prvozpracovatel) nebo informaci, kterou přijal ke zpracování od externích subjektů, zařadit do jedné ze čtyř kategorií klasifikace informací a dokument s informací řádně označit v souladu se zvolenou kategorií. Zaměstnanec označí jen ten dokument, který již není označen ze strany MPSV, GŘ ÚP ČR, jiného útvaru ÚP ČR, případně agendového informačního systému. Definované kategorie a způsob jejich značení je popsán v přílohách příkazu ministra č. 27/2007 a č. 23/2012.

2. Veškeré informace musí být zařazeny do kategorie. Typ zvolené kategorie závisí na charakteru informace. Dělení informací do kategorií provádí prvozpracovatel informace nebo zaměstnanec, který informaci (dokument) přijal ke zpracování od externích subjektů. Prvozpracovatel je typicky zaměstnanec, který informaci (dokument) vytvořil. Pokud informace obsahuje skutečnosti náležící do různých kategorií, musí být jako celek zařazena do kategorie s nejvyšším stupněm ochrany. Definované kategorie informací jsou řazeny podle stupně ochrany (1 určuje nejvíce chráněné informace, 4 nejméně): 1. Osobní údaje, 2. Chráněné informace, 3. Informace pro vnitřní potřebu, 4. Informace určené pro zveřejnění.

3. Mezi osobní údaje spadají veškeré informace, které je organizace povinna chránit ve smyslu § 4 zákona č.101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Do kategorie osobních údajů budou zařazeny také citlivé údaje definované § 4 zákona č.101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Veškeré osobní údaje budou chráněny stejně, jako kdyby se jednalo o údaje citlivé. „Osobním údajem“ se rozumí jakákoliv informace týkající se fyzické osoby, jestliže lze na jejím základě přímo či nepřímo zjistit její identitu, zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro

fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a jejich likvidace. Likvidací osobních údajů se rozumí fyzické zničení všech nosičů obsahující likvidované osobní údaje nebo, je-li to účelné a možné, jejich fyzické vymazání ze všech nosičů, na kterých jsou obsaženy. Informace, která nebude zařazena mezi osobní údaje, bude klasifikována jednou z kategorií definovaných dále.

4. Do kategorie „chráněné informace“ se informace zařazuje v případě, že její vyzrazení, a to i uvnitř organizace, ztráta, chybné použití, neoprávněná modifikace nebo přístup neoprávněné osoby k ní, a to úmyslně i z nedbalosti, mohou závažně ohrozit či ztížit činnost organizace, mít závažné negativní právní důsledky pro organizaci, například způsobit újmu fyzické nebo právnické osobě nebo osobě které se informace týká, přičemž se tato osoba může domoci náhrady za tuto újmu.

5. Do kategorie „informace pro vnitřní potřebu“ se informace zařazuje v případě, že svým obsahem nespadá do kategorie „chráněné informace“ nebo do kategorie „určené pro zveřejnění“. Jedná se zejména o informaci vzniklou při přípravě rozhodnutí, a to do doby, kdy příprava končí rozhodnutím, informace vztahující se výlučně k vnitřním pokynům a další informace, které orgán veřejné správy podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, neposkytne nebo může omezit jejich poskytnutí. Do kategorie „pro vnitřní potřebu“ se informace zařazuje rovněž v případě, že svým obsahem nespadá do kategorie „chráněné informace“ a zároveň zvláštní zákon neumožňuje její zveřejnění nebo v určitých případech umožňuje odepřít její zpřístupnění (např. informace se týká dosud nezpracovaných nebo nevyhodnocených údajů).

6. Do kategorie „informace určené pro zveřejnění“ se informace zařazuje v případě, kdy se jedná o informaci, kterou je orgán veřejné správy povinen zveřejnit podle zvláštního zákona, např. zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů nebo o informaci, o jejímž zveřejnění organizace rozhodne (tisková prohlášení, informativní materiály, nabídky pracovních příležitostí apod.).

7. Aby bylo možné zajistit patřičnou ochranu informací, je nutné informace klasifikovat a následně označit. Všichni zaměstnanci jsou povinni nově vytvářené informace / data zařadit do jedné ze čtyř kategorií a informace řádně označit v souladu se zvolenou kategorií. Vzhledem k tomu, že je většina informací zařazena do kategorie „pro vnitřní potřebu“, nebude u této kategorie označení klasifikace vyžadováno (veškeré informace které nebudou označeny, budou automaticky náležet do kategorie „pro vnitřní potřebu“). Informace v tištěné podobě budou označeny vždy v záhlaví nebo zápatí přední strany prvního listu dokumentu. V netištěné podobě (datový nosič informace) bude označení uvedeno na popisném štítku, obálce, obalu a podobně. Rovněž v případě zobrazení informace na obrazovce počítače musí být informace příslušným způsobem označena nebo musí být zaměstnanci, kterému se informace zobrazila prokazatelně známo, do které kategorie je informace zařazena. Informace určené pro zveřejnění nemusí být označeny při vlastním zveřejnění informace, kdy je samotným aktem zveřejnění patrné, že se jedná o veřejnou informaci (například zveřejněním informace na internetu, v tisku, a podobně). Informace budou označovány následovně:

- Osobní údaje jsou značeny slovy „Osobní údaje“ nebo zkratkou „OSÚ“.
- Chráněné informace jsou značeny slovy „Chráněné informace“ nebo zkratkou „CH“.
- Informace pro vnitřní potřebu nejsou označeny vůbec nebo jsou značeny slovy „Pro vnitřní potřebu“ nebo zkratkou „VP“.
- Informace určené pro zveřejnění jsou do doby zveřejnění značeny slovy „Veřejné“ nebo zkratkou „VEŘ“.

Článek III
Použití kamerových systémů

1. Krajská pobočka je v případě použití kamerových systémů se záznamem, v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „zákon“), správcem osobních údajů. Zpracovatelem může být např. externí bezpečnostní agentura; na zpracovatele se vztahují povinnosti správce tam, kde tak stanoví zákon.

2. Krajská pobočka jako správce zpracovává osobní údaje z kamerového systému bez souhlasu subjektů, a to na základě výjimky dle § 5 odst. 2 písm. e) zákona, tj. z důvodu nezbytnosti pro ochranu práv a právem chráněných zájmů správce, takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Ochranou práv a právem chráněných zájmů správce se míní zejména ochrana života a zdraví zaměstnanců správce, ochrana života a zdraví klientů správce, ochrana majetku ve smyslu § 14 odst. 3 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, ochrana související s výplatou dávek v hotovosti (např. podle zákona č. 111/2006 Sb., o pomoci v hmotné nouzi) a další. Dále se ochranou práv a právem chráněných zájmů míní také ochrana informačních systémů správce resp. MPSV a jejich dat, které obsahují osobní údaje fyzických a právnických osob, včetně citlivých údajů, a ochrana související s činností správce podle zákona č. 240/2000 Sb., krizový zákon.

3. Shromažďované osobní údaje musí odpovídat pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.

4. Správce uchovává osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.

5. Osobní údaje se shromažďují pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti.

6. Při zpracování osobních údajů správce dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

7. Při zpracování osobních údajů je správce povinen bez zbytečného odkladu subjekt údajů informovat o zpracování jeho osobních údajů, činí tak mj. informačními cedulemi na budovách resp. v místech použití kamerového systému. Správce je dále při shromažďování osobních údajů povinen subjekt údajů informovat o tom,

v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona. Tato povinnost je naplněna zveřejněním tohoto dodatku směrnice (resp. jeho příloh) v příslušných budovách a na internetových stránkách¨.

8. Požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat v rozsahu dle § 12 zákona.

9. Správce je povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů. Toto je plněno formou omezeného přístupu (z hlediska personálního i technického) k záznamům z kamerového systému.

10. Zaměstnanci správce a jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

11. Správce, nebo na základě jeho pokynu zpracovatel, je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů podle § 21 zákona. Tato likvidace probíhá automaticky po uplynutí stanovené doby přepisem záznamů.

12. Úřad práce, pokud hodlá zpracovávat osobní údaje nebo změnit již registrované zpracování, je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů (ÚOOÚ) ve smyslu § 16 zákona, a to před zpracováváním osobních údajů.

13. V souladu s § 316 odst. 2 zákona č. 262/2006 Sb., zákoník práce, zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování. V tomto smyslu zaměstnavatel nepodrobuje sledování prostory s vyšší mírou soukromí (toalety, kuchyňky apod.) a nepodrobuje nepřetržitému sledování ani stálá pracoviště zaměstnanců (ve smyslu kancelářských prostor). Pokud je kamerový systém na chodbách či výjimečně místnostech s přepážkami, jsou dány důvody jako zvláštní činnost zaměstnavatele uvedené v bodě 4 tohoto dodatku, případně jde o sledování online a se záznamem pouze v krizové situaci (incidenční záznam).

14. Dotčenými subjekty jsou klienti úřadu práce, návštěvníci úřadu práce a zaměstnanci úřadu práce. Základními právy dotčených subjektů jsou:

- aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti,
- právo na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů,
- na informování, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny,
- na informování o zpracování svých osobních údajů a poskytnutí informace od správce,
- požádat správce nebo zpracovatele o vysvětlení nebo aby správce nebo zpracovatel odstranil vzniklý stav, pokud subjekt zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování.

15. Za plnění povinností v oblasti kamerových systémů odpovídají jednotlivá kontaktní pracoviště s kamerovým systémem. Útvary kanceláře krajské pobočky (oddělení správy majetku a investic, oddělení informatiky) a odbor kontrolně právní krajské pobočky (oddělení právní), jim poskytují v nezbytných případech (instalace systému, komunikace s ÚOOÚ apod.) součinnost.

16. Přílohy této směrnice určují jednotlivé budovy, kde správce instaloval kamerový systém a obsahují zejména:
    a) název kontaktního pracoviště, adresu budovy,
    b) informaci o umístění kamerového systému,
    c) číslo registrace u ÚOOÚ, pokud je potřeba,
    d) informaci o případném zpracovateli osobních údajů,
    e) prostředky a způsob zpracování osobních údajů; kdo a jakým způsobem bude údaje zpracovávat a komu mohou být údaje zpřístupněny,
    f) dobu uchovávání osobních údajů,
    g) přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů.

Ukládám kanceláři krajské pobočky uveřejnit směrnici na SharePointu a vedoucím zaměstnancům seznámit prokazatelně se směrnicí všechny zaměstnance bez zbytečného odkladu.

Tato směrnice je závazná pro všechny zaměstnance Krajské pobočky v Plzni vč. kontaktních pracovišť

Příloha – kamerové systémy

č. 1

a) Krajská pobočka v Plzni, KoP v Plzni, KoP Plzeň-sever, KoP Plzeň-jih, **budova Kaplířova 7, Plzeň**

b) Kamerový systém v počtu 12 kamer s umístěním: 1 - hlavní vchod ze vstupní haly, 2 – čekárna odd. ZAM – přízemí, pravá strana, 3 – chodba 1.p., pravá strana, 4 – garáž, suterén, 5 – nádvoří za budovou ÚP – venkovní kamera, 6 – chodba přízemí, pravá strana, 7 – chodba 1.p., levá strana, 8 – parkoviště před budovou ÚP – venkovní kamera, 9 – hlavní vchod do ÚP – venkovní kamera, 10 – parkoviště a závora na nádvoří za budovou, 11 – velké parkoviště a závora za budovou ÚP, 12 – zadní část budovy ÚP s přístřeškem na parkovišti. Kamery jsou se záznamem.

c) Číslo registrace ÚOOÚ: 00003374.

d) Zpracovatelem údajů je smluvní bezpečnostní agentura Securitas ČR s.r.o. (resp. její zaměstnanci) na základě uzavřené smlouvy a správce.

e) Kamerový systém má záznamové zařízení s HDD uložené na ve vrátnici. Na záznamovém zařízení se uchovávají nahrané záznamy. Nahrávky jsou přístupné jmenovitě uvedeným zaměstnancům smluvní bezpečnostní agentury, kteří pracují v budově ÚP a ze zaměstnanců ÚP: ředitelům KrP a příslušných KoP a jejich zástupcům, vedoucímu kanceláře KrP, vedoucí referátu správy majetku a investic KrP, zaměstnancům útvaru informatiky. V případě potřeby by mohl být záznam předán Policii ČR nebo městské policii.

f) Doba uchovávání údajů je 5 pracovních dnů. Po této době se údaje automaticky likvidují, resp. zničí novým záznamem.

g) Technicko-organizační opatření k zajištění ochrany osobních údajů jsou:
- zařízení je umístěno v místnosti s omezeným vstupem, zajištěné zámky
- mimo pracovní dobu je budova napojena na centrální pult ochrany Policie ČR
- přístupová práva pro omezený počet zaměstnanců

č. 2

a) Krajská pobočka v Plzni, KoP v Plzni, KoP Plzeň-sever, KoP Plzeň-jih, **budova Klatovská 200e, Plzeň**

b) Kamerový systém v počtu 14 kamer s umístěním: 1 – nádvoří a vchod – venkovní kamera, 2 – vestibul přízemí, 3 - chodba přízemí, levá strana, 4 – čekárna přízemí – soc. dávky, 5 – chodba přízemí, levá strana před čekárnou, 6 – chodba přízemí, levá strana za čekárnou, 7 – chodba přízemí, pravá strana, 8 – vestibul 1.p., 9 – chodba 1.p., levá strana, 10 – chodba 1.p., pravá strana, 11 – vestibul 2.p., 12 – chodba 2.p., levá strana, 13 – chodba 2.p., pravá strana, 14 – boční rampa, vchod do suterénu – venkovní kamera Kamery jsou se záznamem.

c) Číslo registrace ÚOOÚ: 00037548.

d) Zpracovatelem údajů je smluvní bezpečnostní agentura Securitas ČR s.r.o. (resp. její zaměstnanci) na základě uzavřené smlouvy a správce.

e) Kamerový systém má záznamové zařízení uložené na PC ve vrátnici. Na záznamovém zařízení se uchovávají nahrané záznamy. Nahrávky jsou přístupné jmenovitě uvedeným zaměstnancům smluvní bezpečnostní agentury, kteří pracují v budově ÚP a ze zaměstnanců ÚP: ředitelům KrP a příslušných KoP a jejich zástupcům, vedoucímu kanceláře KrP, vedoucí referátu správy

majetku a investic KrP, zaměstnancům útvaru informatiky. V případě potřeby by mohl být záznam předán Policii ČR nebo městské policii.

f) Doba uchovávání údajů je 5 pracovních dnů. Po této době se údaje automaticky likvidují, resp. zničí novým záznamem.

g) Technicko-organizační opatření k zajištění ochrany osobních údajů jsou:
   - zařízení je umístěno v místnosti s omezeným vstupem, zajištěné zámky
   - mimo pracovní dobu je budova napojena na centrální pult ochrany Policie ČR
   - přístupová práva pro omezený počet zaměstnanců

č. 3

a) Krajská pobočka v Plzni, KoP Rokycany, **budova Palackého 162, Rokycany**

b) Kamerový systém v počtu 2 kamer je umístěn: 1 - v přízemí budovy ve směru na hlavní vchod, 2 - v 1. patře budovy ve směru na schodiště. Kamery jsou se záznamem, ale pouze v době napojení budovy na EZS (mimo pracovní dobu).

c) Číslo registrace ÚOOÚ: 00041135/002.

d) Osobní údaje zpracovává správce.

e) Kamerový systém má záznamové zařízení uložené v serverovně KoP. Na záznamovém zařízení se uchovávají nahrané záznamy. Nahrávky jsou přístupné zaměstnancům útvaru informatiky, ředitelce KoP a její zástupkyni. V případě potřeby by mohl být záznam předán Policii ČR nebo městské policii.

f) Doba uchovávání údajů je 5 pracovních dnů. Po této době se údaje automaticky likvidují, resp. zničí novým záznamem.

g) Technicko-organizační opatření k zajištění ochrany osobních údajů jsou:
   - zařízení je umístěno v kanceláři s omezeným vstupem, zajištěné zámky
   - mimo pracovní dobu je budova napojena na centrální pult ochrany Policie ČR
   - přístupová práva pro omezený počet zaměstnanců
   - záznam je prováděn pouze v době, kdy je EZS budovy uveden v činnost, tzn. není v budově nikdo přítomen. Osobní údaje jsou zaznamenány jen v případě, kdy dojde k neoprávněnému vstupu do budovy bez odkódování EZS.

č. 4

a) Krajská pobočka v Plzni, KoP Tachov, **budova Tř. Míru 1633, Tachov**

b) Kamerový systém v počtu 5 stacionárních kamer je umístěn takto:
   - 2 kamery se záznamovým zařízením v kancelářích č. 4 a 8 v přízemí budovy, kamery snímají prostor před odbavovacími přepážkami,
   - 3 kamery bez záznamového zařízení (v režimu on-line), z toho dvě v odbavovací hale a jedna na chodbě před odbavovací halou v přízemí budovy; kamery mohou být přepnuty do režimu záznamu v případě incidentu.

c) Číslo registrace ÚOOÚ: 00041135/003.

d) Osobní údaje zpracovává správce.

e) Monitoring z kamer v režimu on-line je přístupný řediteli KoP, vedoucím oddělení NSD a zaměstnanosti a zaměstnankyni sekretariátu. Po pracovní době jsou do režimu záznamu zapojeny všechny kamery. Kamerový systém má záznamové zařízení uložené v kanceláři u správce sítě. Na záznamovém zařízení se uchovávají nahrané záznamy. Nahrávky jsou přístupné ředitelce KoP a jejímu zástupci, zaměstnancům útvaru informatiky a vedoucímu NSD. V případě potřeby by mohl být záznam předán Policii ČR nebo městské policii.

f) Doba uchovávání údajů jsou 2 pracovní dny. Po této době se údaje automaticky likvidují, resp. zničí novým záznamem.

g) Technicko-organizační opatření k zajištění ochrany osobních údajů jsou:
   - záznamové zařízení je umístěno v uzamčené místnosti, zajištěné zámky,
   - mimo pracovní dobu je budova napojena na centrální pult ochrany Policie ČR,
   - přístupová práva pro omezený počet zaměstnanců,
   - dokumentace k přijatým technicko-organizačním opatřením.

č. 5

a) Krajská pobočka v Plzni, KoP Klatovy, **budova Voříškova 825/III, Klatovy**
b) Kamerový systém v počtu 11 stacionárních kamer je umístěn takto:
   - hlavní vchod ze vstupní haly
   - vchod (vnitřní) do přístavby
   - chodba oddělení zaměstnanosti
   - pokladna (není v provozu)
   - chodba IPS (informační a poradenské středisko)
   - boční vchod do budovy (pohledem zevnitř)
   - chodba v přízemí
   - schodiště v 1. patře
   - schodiště ve 2. patře
   - schodiště ve 3. patře
   - schodiště ve 4. patře
c) Číslo registrace ÚOOÚ: 00041135/008
d) Osobní údaje zpracovává správce.
e) Kamerový systém má záznamové zařízení uložené v serverovně KoP. Na záznamovém zařízení se uchovávají nahrané záznamy. Nahrávky jsou přístupné pouze zaměstnancům útvaru informatiky a ředitelce KoP. V případě potřeby by mohl být záznam předán Policii ČR nebo městské policii.
f) Doba uchovávání údajů jsou 2 pracovní dny. Po této době se údaje automaticky likvidují, resp. zničí novým záznamem.
g) Technicko-organizační opatření k zajištění ochrany osobních údajů jsou:
   - záznamové zařízení je umístěno v uzamčené místnosti, zajištěné zámky,
   - mimo pracovní dobu je budova napojena na centrální pult ochrany
   - přístupová práva pro omezený počet zaměstnanců.