KARLOVARSKÝ KRAJ
ŘEDITELKA KRAJSKÉHO ÚŘADU

S M Ě R N I C E

ŘEDITELKY KRAJSKÉHO ÚŘADU

č. SE 04/2018

ZPRACOVÁNÍ A OCHRANA OSOBNÍCH ÚDAJŮ

Zpracovatel:	**Mgr. Daniel Tovth, vedoucí odboru kancelář ředitelky úřadu**	
Rozsah působnosti:	**krajský úřad**	
Nabývá účinnosti:	***Počet stran:***	***Počet příloh:***
1. 10. 2018	**15**	**3**

Tímto předpisem se ruší předpis číslo:	**SE 02/2012**

Originál předpisu je uložen:	**odbor legislativní a právní a krajský živnostenský úřad**
Elektronická podoba předpisu je uložena na	**portál úředníka krajského úřadu**
Předpis je zveřejněn na internetových stránkách Karlovarského kraje	

Za odbor legislativní a právní a krajský živnostenský úřad schválil:	**PhDr. Mgr. Vratislav Smoleja, vedoucí odboru legislativního a právního a krajského živnostenského úřadu**
Vydal:	**Mgr. Martina Vránová, ředitelka krajského úřadu**

Obdrží:	**všichni vedoucí odborů krajského úřadu**

Obsah

V souladu s ustanovením §69 odst. 2 písm. f) zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů, vydávám tuto

s m ě r n i c i :

Čl. I.
Úvodní ustanovení

1. Směrnice pro zpracování a ochranu osobních údajů upravuje technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s nařízením Evropského parlamentu a rady (EU)[1] (dále jen „nařízení“) s cílem zajištění jednotného postupu při ochraně osobních údajů v podmínkách Krajského úřadu Karlovarského kraje (dále také „krajský úřad“ a „kraj“).

2. Správcem osobních údajů (dále jen „správce“) ve smyslu směrnice je kraj, v podmínkách krajského úřadu zastupuje správce ředitelka krajského úřadu.

3. Směrnice je závazná pro všechny zaměstnance kraje zařazené do krajského úřadu (dále jen „zaměstnanec“) včetně osob konajících práci na základě dohod o pracích konaných mimo pracovní poměr.

Čl. II.
Výklad některých pojmů a zkratek

1. ***Zpracování*** je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, která je prováděna 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.

2. ***Osobní údaje*** jsou 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.

3. ***Správcem kamerového systému*** je vedoucí odboru kancelář ředitelky úřadu, který odpovídá kraji za dodržování veškerých zásad uvedených v pokynech k ochraně osobních údajů v příslušném kamerovém systému.

4. ***Zpracovatel***[2] je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, která zpracovává osobní údaje pro kraj.

5. ***Příjemcem*** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterému jsou osobní údaje poskytnuty či zpřístupněny, 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 právem členského státu, se za příjemce nepovažují. Zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany osobních údajů pro dané účely zpracování. Za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly,

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[2] Článek 28 nařízení.

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.

6. ***Souhlas*** subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

7. ***Pověřenec*** pro ochranu osobních údajů (dále jen „pověřenec“) je pozice v rámci krajského úřadu, v níž působí zaměstnanec nebo externí pracovník jako ochránce osobních údajů subjektů.

8. ***Dozorový úřad*** je pro potřeby této směrnice Úřad pro ochranu osobních údajů.

9. ***Vedoucí zaměstnanci*** jsou pro účely této směrnice vedoucí jednotlivých oddělení a vedoucí odborů.

10. ***Oprávněnou osobou*** je pro účely této směrnice:
    a) zaměstnanec, který v rámci plnění povinností plynoucích mu z pracovní náplně má přístup k osobním údajům a dále je zpracovává,
    b) osoba, které na základě smluvního vztahu má správcem povolený přístup k osobním údajům.

11. ***Zvláštní kategorie osobních údajů***[3] (tzv. citlivé údaje) 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.

12. ***Ostatními zaměstnanci*** jsou zaměstnanci, kteří mohou přijít do styku s osobními údaji, ale tyto údaje dále nezpracovávají.

13. ***Věcně příslušným odborem*** je odbor či samostatné oddělení krajského úřadu, který je věcně příslušný ke zpracování osobních údajů (na základě zvláštního zákona, Organizačního řádu nebo rozhodnutí ředitelky krajského úřadu). Vedoucí věcně příslušného odboru je správcem osobních údajů v působnosti tohoto odboru.

14. ***Bezpečnostní událost*** je situace, kdy mohlo dojít k selhání některého z bezpečnostních opatření a tím mohlo dojít k porušení zabezpečení ochrany osobních údajů.

15. ***Bezpečnostní incident*** je situace, kdy došlo k selhání některého z bezpečnostních opatření a tím došlo k porušení zabezpečení ochrany osobních údajů.

Čl. III.
Vymezení odpovědnosti

1. Pověřenec dohlíží na zpracování a ochranu osobních údajů u správce a plní další povinnosti při zpracování a ochraně osobních údajů

2. Vedoucí zaměstnanci odpovídají za zpracování a ochranu osobních údajů v rozsahu své působnosti.[4]

3. Oprávněné osoby odpovídají za zpracování a ochranu osobních údajů ve zpracovatelských operacích (agendách a činnostech).

[3] Článek 4 odst. 13, 14 a 15 nařízení.
[4] Řád ředitelky krajského úřadu č. R 02/2018, Organizační řád.

Čl. IV.
Úkoly a činnosti pověřence

1. Pověřenec je v pozici v rámci krajského úřadu jako ochránce osobních údajů klientů krajského úřadu, zaměstnanců apod.

2. Pověřenec je přímo podřízen ředitelce krajského úřadu.

3. Funkci pověřence vykonává úředník zařazený do odboru kanceláře ředitelky úřadu.

4. Pověřenec vykonává níže uvedené hlavní úkoly:
   a) poskytuje zaměstnavateli a ostatním zaměstnancům informace a poradenství o jejich povinnostech podle nařízení a dalších předpisů v oblasti ochrany osobních údajů,
   b) monitoruje soulad s nařízením, dalšími právními předpisy a vnitřními předpisy a další dokumentací zaměstnavatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců,
   c) poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle čl. 35 nařízení,
   d) spolupracuje s dozorovým úřadem,
   e) působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl. 36 nařízení, a případně vedení konzultací v jakékoli jiné věci,
   f) působí jako kontaktní osoba zaměstnavatele pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle nařízení.

5. Mezi další činnosti a oprávnění pověřence patří:
   a) být náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů, mít plný přístup ke všem souvisejícím činnostem krajského úřadu, informacím, dokladům, systémům, operacím a záznamům,
   b) vyžadovat od vedoucích odborů a oprávněných osob potřebnou součinnost a jednat se všemi vedoucími a ostatními zaměstnanci bez ohledu na jejich postavení v hierarchii řízení,
   c) zajišťovat ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a taktéž oznamovat případy porušení zabezpečení osobních údajů subjektům údajů dle nařízením stanovených lhůt,
   d) vést evidenci o všech případech porušení zabezpečení osobních údajů v rozsahu dle nařízení[5],
   e) informovat, radit a vydávat doporučení v oblasti zpracování a ochrany osobních údajů oprávněným osobám,
   f) vyžadovat kontrolní nebo auditní zprávy vypracované externími kontrolními orgány,
   g) mít plný přístup ke sledování plnění opatření k nápravě nedostatků zjištěných činností DPO,
   h) provedená opatření dokumentovat ve formě zpráv a přiměřeným způsobem vést evidenci realizovaných konzultací; jednotlivá ověření jsou realizována na základě pověření ředitelky krajského úřadu; postup oznámení zahájení ověření a projednání zprávy z ověření je realizován obdobným způsobem jako postup oznámení zahájení interního auditu a projednání zprávy z interního auditu,
   i) předkládat ředitelce krajského úřadu zprávy z provedených ověření, průběžně ji informovat o průběhu ověření a neprodleně jí předávat informace o závažných zjištěních učiněných při výkonu své funkce,

[5] Článek 33 odst. 3 nařízení.

j) navrhovat ředitelce krajského úřadu přijetí doporučení k nápravě nedostatků zjištěných v rámci činnosti pověřence,

k) každoročně do 31. ledna předkládat ředitelce krajského úřadu souhrnnou roční zprávu o činnosti pověřence a současně přihlížet k povaze, rozsahu, kontextu a účelům zpracování,

l) zachovávat obezřetnost, diskrétnost a mlčenlivost při používání a ochraně informací získaných činností pověřence, při práci s utajovanými skutečnostmi a osobními údaji postupovat v souladu s příslušnými předpisy,

m) zabezpečit veškeré potřebné podklady pro vypracování zprávy z vykonaného šetření, pro dokladování zjištění a z nich vyplývajících závěrů a navazujících doporučení,

n) koordinovat výkon práv subjektů údajů a zajišťovat jejich informovanost o průběhu a řešení jejich požadavků na uplatnění práva do stanovené lhůty,

o) do 31. ledna každého roku připravit plán činnosti pověřence a s tímto nejpozději do 15. února seznámit ředitelku krajského úřadu, (plán činnosti se může v průběhu roku upravovat, zejména v návaznosti na nově vzniklé situace v oblasti ochrany osobních údajů)

p) prostřednictvím vedoucích zaměstnanců informovat o poznatcích z kontrolní činnosti v dané oblasti,

q) ve spolupráci s vedoucími odborů vést dokumentaci záznamů o činnostech zpracování,

r) monitorovat a případně aktualizovat požadavky na zabezpečení osobních údajů,

s) ve spolupráci s ostatními vedoucími zaměstnanci ověřovat, zda jsou stávající technická a organizační opatření dostatečná, případně předkládat ředitelce krajského úřadu návrhy k úpravě stávajících opatření,

t) ve spolupráci s vedoucím odboru kancelář ředitelky úřadu činí kroky k zavedení dané problematiky do plánů vzdělávání,

u) rozvíjet znalosti a metodicky vést vzdělávání zaměstnanců zpracovávajících osobní údaje z problematiky zpracování a ochrana osobních údajů.

Čl. V.
Povinnosti vedoucích zaměstnanců

1. Vedoucí věcně příslušného odboru je povinen při zpracovávání osobních údajů, kdy je kraj v pozici správce nebo zpracovatele osobních údajů, zajistit nastavení vhodných technických opatření (nastavení přístupových práv, zabezpečení listin, spisů apod.) na příslušném odboru vzhledem k charakteru a množství zpracovávaných osobních údajů.

2. Vedoucí věcně příslušného odboru shromažďuje aktuální podklady k oprávněnosti účelů zpracování osobních údajů na příslušném odboru v Přehledu účelů zpracování osobních údajů, který je uveden v příloze č. 1 směrnice a tyto předává při jakékoliv aktualizaci pověřenci.

3. Vedoucí věcně příslušného odboru ve spolupráci s pověřencem zodpovídá za vedení záznamů o činnostech zpracování.

4. Vedoucí věcně příslušného odboru zodpovídá za to, aby k dokumentům a spisům s osobními údaji zpracovávaných na daném odboru měly přístup pouze oprávněné osoby, a to vždy jen za příslušnou oblast zpracování.

5. Vedoucí věcně příslušného odboru zodpovídá za součinnost odboru potřebnou ke splnění informační povinnosti a k ověření správnosti a úplnosti záznamů o jimi prováděných činnostech zpracování.

6. Vedoucí věcně příslušného odboru zodpovídá za poskytnutí informací o nových zpracováních nebo změnách dosavadních, a to prostřednictvím aplikace ServiceDesk nejméně 20 pracovních dnů před

začátkem tohoto zpracování. Vedoucí věcně příslušného odboru následně doplní Přehled účelů zpracování osobních údajů a tento bezprostředně předá pověřenci.

7. Vedoucí věcně příslušného odboru zajistí v součinnosti s pověřencem výkon práv subjektu údajů.

8. Vedoucí věcně příslušného odboru ihned po zjištění prostřednictvím aplikace ServiceDesk oznámí pověřenci porušení nebo podezření na porušení zabezpečení osobních údajů, zánik již existující zpracovatelské operace nebo změnu v příslušném právním předpise, který je právním důvodem pro zpracování osobních údajů.

9. Vedoucí věcně příslušného odboru je povinen stanovit oprávněné osoby ke zpracování osobních údajů včetně rozsahu a způsobu zpracování osobních údajů (v rámci pracovní náplně zaměstnance).

10. Vedoucí věcně příslušného odboru kontroluje dodržování zásad nakládání s osobními údaji na příslušném odboru a plnění archivačních a skartačních lhůt dle Spisového řádu[6].

11. Vedoucí zaměstnanec zodpovídá za prokazatelné seznámení svých podřízených zaměstnanců s jejich konkrétními povinnostmi při zpracovávání a ochraně osobních údajů v rámci agend a činností vykonávaných v souladu s pracovní náplní.

12. Vedoucí zaměstnanec dále stanoví ve spolupráci s odborem informatiky krajského úřadu rozsah přidělení uživatelských oprávnění do aplikací a datových zdrojů pro své podřízené, a to v rozsahu nezbytně nutném pro plnění pracovních povinností (například přístup k osobním údajům na společných úložištích – disk K - a podobně).

13. Vedoucí zaměstnanec zabezpečí, aby dokumenty, které jsou zveřejňovány např. dálkovým přístupem, obsahovaly pouze takové osobní údaje, které vyžaduje nebo umožňuje zvláštní zákon, dle kterého ke zveřejnění dochází.

14. Vedoucí odboru kancelář ředitelky úřadu zajistí 1x ročně realizaci povinného školení zaměřeného na problematiku ochrany osobních údajů.

15. Vedoucí odborů zajistí účast zaměstnanců v rámci jejich průběžného vzdělávání na školení zaměřené k dané problematice, organizovaných odborem kanceláře ředitelky úřadu, oddělením personálních věcí a vzdělávání.

Čl. VI.
Povinnosti oprávněných osob

1. Oprávněné osoby jsou povinny dodržovat pravidla stanovená v nařízení, v zákonech upravujících ochranu osobních údajů[7], v této směrnici a v dalších vnitřních předpisech kraje a řídit se pokyny vedoucích zaměstnanců, případně i pověřence.

2. Oprávněné osoby, kterým bylo přiděleno přístupové oprávnění do některého z neveřejných informačních systémů, jsou povinny využívat zjištěné údaje výlučně k plnění pracovních povinností a dodržovat závazná pravidla, vydaná správci těchto systémů, požadavky zvláštních zákonů i povinnosti stanovené touto směrnicí.

3. Oprávněné osoby jsou povinny v rámci plnění svých pracovních povinností plnit i opatření k ochraně osobních údajů dle nařízení[8], zejména:

[6] Řád ředitelky krajského úřadu č. R02/2011, Spisový a skartační řád.
[7] Např. § 15 odst. 3 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.
[8] Článek 5 odst. 1 nařízení.

a) zpracovávat osobní údaje za podmínek a v rozsahu jim stanoveném v souladu s platnými přístupy do informačních systémů a SW aplikací,

b) osobní údaje shromažďovat a dále zpracovávat v rozsahu nezbytně nutném, není-li rozsah zpracovávaných osobních údajů stanoven pro konkrétní účel (agendu) zvláštním zákonem,

c) při shromažďování osobních údajů přímo od subjektů údajů shromažďovat osobní údaje pouze otevřeně, tj. neshromažďovat osobní údaje skrytě nebo pod záminkou jiného účelu,

d) při zpracování osobních údajů

- zpracovávat pouze přesné osobní údaje s ohledem na účel zpracování; v případě zjištění, že zpracovávané osobní údaje nejsou přesné, zpracování zablokovat do doby jejich opravy nebo doplnění, jinak osobní údaje zlikvidovat na základě pokynu správce,
- zpracovávat osobní údaje pouze k účelům, k nimž byly shromážděny (k jinému účelu pouze v případě, že fyzická osoba, ke které se osobní údaje vztahují, dala k tomu předem souhlas),
- nesdružovat osobní údaje získané k rozdílným účelům,
- uchovávat osobní údaje pouze po dobu, která je nezbytně nutná k účelu zpracování; pominul-li účel zpracování konkrétních osobních údajů postupovat v souladu se Spisovým a skartačním řádem, případně údaje zlikvidovat na základě pokynu správce,

e) ukládat nosiče obsahující osobní údaje, a to v listinné i elektronické podobě na náležitě zajištěná místa (uzamykatelné skříně, kartotéky apod.); při práci s nosiči postupovat tak, aby jiná osoba nemohla zneužít tyto nosiče jako zdroj informace (dle zásad „čistého stolu“ a „prázdné obrazovky“); elektronické datové soubory obsahující osobní údaje je možné uchovávat v paměti počítače pouze, je-li přístup k takovýmto souborům chráněn heslem nebo je-li přístup k užívání počítače, v jehož paměti jsou tyto soubory umístěny, chráněn heslem,

f) nepořizovat kopie nosičů s osobními údaji či osobních údajů samých pro jinou než pracovní potřebu a ani to umožňovat jiným; s takovými kopiemi nakládat stejně jako s originálem,

g) neumožnit zpracování osobních údajů jiné osobě, která není pro konkrétní účel zpracování oprávněnou osobou (například neprodleně po vytištění odebírat dokumenty obsahující osobní údaje z tiskáren, kopírek nebo faxů),

h) zpracovávané zvláštní kategorie osobních údajů poskytnout pouze těm oprávněným osobám, které tyto údaje potřebují pro plnění svých pracovních povinností,

i) provádět průběžné znehodnocování podkladových materiálů s osobními údaji (rukopisů, konceptů, poznámek) sloužících ke zpracování dokumentů a to použitím odpovídajících technických a SW prostředků (např. skartovací stroj),

j) osobní údaje (v listinné i elektronické formě) předávat

- v rámci krajského úřadu pouze oprávněným osobám způsoby stanovenými Spisovým a skartačním řádem,
- mimo krajský úřad pouze v případech plynoucích z působnosti kraje a krajského úřadu (dle zásad uvedených ve Spisovém a skartačním řádu), stanoví-li tak zvláštní zákon nebo v souladu s platnou smlouvou v zákonem stanovených mezích,

k) v rámci průběžného vzdělávání se účastnit kurzů zaměřených k problematice ochrany osobních údajů v podmínkách kraje a krajského úřadu,

l) při používání prostředků informačních technologií

- prostředky informačních technologií využívat pouze pro plnění pracovních povinností,
- dodržet stanovené zásady při tvorbě svého přístupového hesla k prostředkům informačních technologií a jednotlivým informačním systémům nebo SW aplikacím (délka, struktura a platnost hesla),
- zachovávat jedinečnost a důvěrnost přístupového hesla, tj. nesdílet heslo s jinou osobou, nezaznamenávat heslo např. na papíře, v souborech v počítači nebo na přenosných médiích,

- heslo změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo vlastního hesla,
- dodržovat zásady bezpečnosti informačních technologií s důrazem na
  i. používání hesel při přihlášení k pracovní stanici, aplikaci či informačnímu systému (ve správě krajského úřadu i ve správě jiných subjektů),
  ii. průběžnou aktualizaci a funkčnost antivirového SW,
  iii. odhlášení při odchodu od pracovní stanice,
- v případě nemožnosti využití centrálního zálohovacího systému (např. data uložená na pevném disku PC) provádět (zabezpečit) zálohování informací obsahujících osobní údaje jinou vhodnou formou (na externí pevný disk, vypálením na CD, DVD, popřípadě na flash disk); s touto zálohou pracovat jako s ostatními nosiči informací obsahujících osobní údaje,
- při používání přenosných prostředků informačních technologií (notebooků) mimo sídlo krajského úřadu
  i. nepředávat tento prostředek třetím osobám,
  ii. učinit všechna dostupná opatření zabraňující případné ztrátě či odcizení přenosného prostředku (neponechávat jej bez dohledu a bez zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.),
  iii. ztrátu či odcizení jakéhokoliv prostředku informačních technologií (notebook, mobilní telefon, flash disk, externí pevný disk, CD č DVD s osobními údaji aj.) neprodleně nahlásit svému nadřízenému a pověřenci prostřednictvím aplikace ServiceDesk,

m) při používání prostředků informačních technologií dodržovat veškeré platné vnitřní předpisy[9],

n) v případě zjištění porušení opatření k ochraně osobních údajů (nebo nabytí podezření) informovat neprodleně svého nadřízeného a pověřence prostřednictvím aplikace ServiceDesk,

o) v zákonných případech osobní údaje anonymizovat; zvýšenou pozornost je třeba věnovat ochraně osobních údajů při ukládání dokumentů na sdílená uložiště (např. disk K),

p) zajistit, aby písemnosti obsahující osobní údaje byly předávány a poskytovány pouze způsoby stanovenými Spisovým skartačním řádem[10],

q) při shromažďování osobních údajů od subjektu údajů vyžadovat jejich souhlas se zpracováním pouze v případě, že nebyl nalezen jiný zákonný důvod[11] pro zpracování těchto osobních údajů,

r) pokud jsou shromažďovány osobní údaje na základě uděleného souhlasu od subjektu údajů, musí být tento subjekt vždy poučen i o možnosti tento souhlas kdykoliv odvolat, a to zasláním žádosti na oficiální e-mailovou adresu nebo poštovní adresu kraje; současně musí být subjekt údajů poučen i o možných následcích jeho odvolání,

s) při zpracovávání osobních údajů subjektu mladšího 18 let v případech, kdy není zpracování stanoveno zvláštním právním předpisem, je oprávněná osoba povinna tak činit se souhlasem a schválením zákonného zástupce – zákonný zástupce subjektu údajů; zároveň vyvine přiměřené úsilí, aby ověřil, že souhlas byl dán opravdu zákonným zástupcem,

t) souhlas musí být písemný a musí být uložen v listinné nebo elektronické podobě, aby byl doložitelný; oprávněná osoba, která souhlas připravuje, je povinna jako výchozí vzor použít souhlas, který je Přílohou č. 2 směrnice.

[9] Např. směrnice ředitelky krajského úřadu č. SE 06/2016, Politika bezpečnosti informací Krajského úřadu Karlovarského kraje.
[10] Řád ředitelky krajského úřadu č. R02/2011.
[11] Článek 6 a 7 nařízení.

Čl. VII.
Bezpečnost osobních údajů

1. Oprávněné osoby i ostatní zaměstnanci jsou povinni v případě zjištění porušení zabezpečení osobních údajů nebo nabytí podezření neprodleně informovat v případě zaměstnanců svého nadřízeného a v případě členů orgánů kraje (členové Zastupitelstva Karlovarského kraje, jednotlivých Výborů Zastupitelstva Karlovarského kraje a Komisí Rady karlovarského kraje) vedoucí odboru kanceláře hejtmanky a vnějších vztahů, kteří ihned po oznámení prostřednictvím aplikace ServiceDesk informují pověřence.

2. Pověřenec na základě hlášení o porušení zabezpečení osobních údajů v součinnosti s příslušným vedoucím zaměstnancem:
   a) vyhodnotí zdroje porušení (interní, externí apod.),
   b) vyhodnotí základní informace o narušení a rozhodne o klasifikaci narušení, tj. zda se jedná o bezpečnostní událost nebo bezpečnostní incident.

3. Pokud je informace vyhodnocena jako bezpečnostní událost, provede pověřenec v rámci dalšího šetření následující kroky:
   a) prověří v záznamech, zda se jedná o nahodilou událost nebo se jedná o událost, která se opakuje,
   b) vypracuje návrh na opatření k nápravě,
   c) návrh na opatření k nápravě předá ředitelce krajského úřadu k posouzení a schválení.

4. Pokud je informace vyhodnocena jako bezpečnostní incident, pověřenec přizve další osoby, které jsou kompetentní pro jeho posouzení, a provedou se následující činnosti:
   a) pokud je to možné, provedou odpovědní zaměstnanci okamžitou nápravu (zastavení provozu, zablokování přístupových oprávnění atd.),
   b) identifikace kategorie porušení:
      - porušení důvěrnosti,
      - porušení dostupnosti,
      - porušení integrity,
   c) identifikace typů osobních údajů, u kterých došlo k porušení bezpečnosti,
   d) stanovení přibližného objemu údajů, u kterých došlo k porušení bezpečnosti,
   e) identifikace pravděpodobného zdroje úniku, či případného porušení zabezpečení osobních údajů,
   f) popis pravděpodobných důsledků dopadů na subjekty údajů,
   g) vyhodnocení rizika dopadů na práva a svobody subjektů údajů:
      - bez rizika,
      - s rizikem,
      - s vysokým rizikem.

5. Po vyhodnocení rizika pověřenec informuje ředitelku krajského úřadu a společně s ní přijme rozhodnutí (o povinnosti ohlášení nebo oznámení) a v případě vyhodnocení:
   a) rizika – provede ohlášení dozorovému úřadu (bez zbytečného odkladu a pokud možno do 72 hodin od zjištění bezpečnostního incidentu),

b) vysokého rizika – provede ohlášení dozorovému úřadu (bez zbytečného odkladu a pokud možno do 72 hodin od zjištění bezpečnostního incidentu) a oznámení subjektům údajů (bez zbytečného odkladu).

6. Dále pověřenec společně s dalšími odpovědnými zaměstnanci vypracuje návrh a odpovědní vedoucí zaměstnanci přijmou a neprodleně zrealizují prvotní možná nápravná opatření ke snížení dopadů na práva subjektů údajů nebo k eliminaci příčiny porušení bezpečnosti osobních údajů.

7. Pověřenec připraví a zpracuje hlášení v souladu s nařízením[12], vždy podle úrovně vyhodnoceného rizika, které po schválení ředitelkou krajského úřadu odešle příslušným subjektům (ohlášení dozorovému úřadu, oznámení subjektům údajů).

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

9. Pověřenec v součinnosti s odpovědnými vedoucími zaměstnanci po odeslání ohlášení provede:
   a) další došetřování incidentu na základě návrhů uvedených v ohlášení dozorovému úřadu,
   b) vypracuje návrh na přijetí dalších nápravných opatření,
   c) kontrolu účinnosti přijatých opatření.

10. Pověřenec společně s dalšími odpovědnými zaměstnanci zpracovává dokumentaci týkající se porušení zabezpečení osobních údajů. Dokumentace musí obsahovat:
    a) veškeré skutečnosti, které se týkají příslušného porušení,
    b) dopady porušení a
    c) přijatá nápravná opatření.

Čl. VIII.
Práva subjektu údajů

1. Výkon práv subjektu údajů u krajského úřadu koordinuje pověřenec v součinnosti s vedoucími zaměstnanci, do jejichž působnosti příslušný požadavek na uplatnění práva spadá.

2. Pro žádosti o uplatnění práv subjektu údajů je zřízeno u Karlovarského kraje jedno vstupní místo, kterým je pověřenec a jehož kontaktní údaje jsou zveřejněny na webových stránkách kraje. V případě doručení žádosti na jiné než vstupní místo dle předchozí věty, je příjemce povinen předat neprodleně tuto žádost pověřenci.

3. Před zahájením vyřizování žádosti o uplatnění práva nejdříve pověřenec dostupnými prostředky ověří totožnost žadatele, který uplatňuje právo, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena oprávněnou osobou prostřednictvím veřejné datové sítě (datovou schránkou fyzické osoby) nebo prostřednictvím kvalifikované služby elektronického doporučeného doručování. V těchto případech odešle pověřenec písemnosti s informacemi o vyřízení nebo řešení žádosti na adresu, ze které byla žádost odeslána. V případě doručení žádosti prostřednictvím poštovní služby odešle pověřenec písemnosti s informacemi o vyřízení nebo předá řešení žádosti do vlastních rukou adresáta/žadatele. V případě osobního předání žádosti ověří pověřenec nebo zaměstnanec, který žádost přijímá, totožnost dle předloženého dokladu totožnosti a současně projedná způsob předání písemnosti s informacemi o vyřízení nebo řešení žádosti. Na danou žádost uvede pozn. „Totožnost ověřena dle *dokladu*“ a přidá svůj podpis.

[12] Článek 33 odst. 3 nařízení.

4. Pokud pověřenec vyhodnotí, že nemá dostatek údajů k řádné identifikaci, informuje o tom žadatele a výkon práva neumožní až do doby doplnění potřebných údajů.

5. Vyřizování probíhá tak, že pověřenec rozešle kopie žádosti o uplatnění práva subjektu údajů všem věcně příslušným vedoucím zaměstnancům k zajištění výkonu práv subjektu údajů. Vedoucí zaměstnanci zajistí realizaci výkonu práv subjektu údajů v součinnosti s pověřencem. Vedoucí zaměstnanci po zajištění výkonu práv subjektu údajů předloží pověřenci do lhůty 14 dnů od sdělení požadavku pověřencem návrh odpovědi, resp. informace o řešení požadavku na uplatnění práva.

6. Subjekt údajů je pověřencem vždy informován o řešení jeho požadavku na uplatnění práva ve stanovené lhůtě, tj. bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Předmětem informace je (jsou):

   a) přijatá opatření, nebo

   b) prodloužení lhůty pro uplatnění příslušného práva (max. o 2 měsíce) a důvody prodloužení této lhůty, nebo

   c) důvody nepřijetí požadovaných opatření a možnost podat stížnost u dozorového úřadu a žádat o soudní ochranu.

7. Informace, veškerá sdělení a provedené úkony na žádost subjektu údajů se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost vždy dokládá správce. V rámci plnění obecné informační povinnosti uveřejněné na internetových stránkách kraje jsou subjekty údajů informovány o jejich právech, včetně práva podat stížnost u dozorového úřadu.

8. Pověřenec eviduje veškeré žádosti o uplatnění práv a způsob jejich vyřízení, včetně odpovědí. O žádosti a způsobu jejího vyřízení pověřenec sepisuje Záznamový list, který je uveden v Příloze č. 3 směrnice. Vedoucí věcně příslušného odboru zajistí předání oznámení všem jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s nařízením[13]. Kopii oznámení zašle vedoucí věcně příslušného odboru pověřenci.

Čl. IX.
Posouzení vlivu zpracování na ochranu osobních údajů

1. Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob, zabezpečí vedoucí daného odboru před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Vedoucí daného odboru v posouzení navrhne plánovaná opatření k řešení rizik, bezpečnostní opatření a mechanismy k zajištění ochrany osobních údajů.[14]

2. Při provádění posouzení vlivu na ochranu osobních údajů si vedoucí daného odboru vždy vyžádá posudek pověřence.

3. Pověřenec konzultuje posouzení vlivu na ochranu osobních údajů před jeho zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.[15]

[13] Článek 16, článek 17 odst. 1 a článkem 18 nařízení.
[14] Článek 35 nařízení.
[15] Článek 36 nařízení.

Čl. X.
Úkony před započetím zpracování osobních údajů

1. Před započetím zpracování osobních údajů uvede oprávněná osoba, ve spolupráci s vedoucím zaměstnancem, účel zpracování a další náležitosti ve formuláři Přehled účelů zpracování osobních údajů, jehož VZOR je přílohou č. 1 směrnice. Účely (důvody) zpracování osobních údajů v jednotlivých agendách vychází ze zvláštních zákonů, nebo jsou osobní údaje zpracovávány na základě vlastního rozhodnutí a poté musí splňovat jeden z důvodů uvedených v nařízení[16].

2. Není-li zpracování osobních údajů nezbytné pro dodržení právní povinnosti nebo ochranu práv a právem chráněných zájmů kraje (krajského úřadu), zajistí zpracovatel před zpracováním osobních údajů souhlas se zpracováním osobních údajů a tento souhlas uchovává po celou dobu zpracování daných osobních údajů.

3. Za souhlas[17] se zpracováním osobních údajů je považováno poskytnutí těchto údajů subjekty osobních údajů:

   a) v listinné podobě s uvedením vlastnoručního podpisu včetně údaje o datu podpisu,

   b) v elektronické podobě s např. připojením elektronického podpisu, se zaškrtnutím příslušného políčka se souhlasem v elektronickém formuláři apod.

4. Souhlas musí být prokazatelný po celou dobu zpracování. V případě, že fyzická osoba souhlas neposkytne, nelze její osobní údaje zpracovávat.

5. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků.

6. V případě zpracování osobních údajů na základě souhlasu, zavede tento souhlas pověřenec do databáze souhlasů na základě podkladů předaných z jednotlivých odborů. Dané podklady budou pověřenci předány nejpozději do 3 dnů od podepsání souhlasu.

7. Subjekt údajů má právo svůj souhlas kdykoliv odvolat.[18] V případě odvolání souhlasu není dále možné osobní údaje zpracovávat, pokud není dán jiný zákonný důvod k jejich zpracování. Odvolání souhlasu bude neprodleně zavedeno oprávněnou osobou do databáze souhlasů.

Čl. XI.
Zpracování zvláštních kategorií osobních údajů

1. Oprávněné osoby nesmí evidovat zvláštní kategorie osobních údajů.

2. Odstavec 1 se nepoužije ve zvláštních případech.[19]

3. Podmínky zpracování zvláštních kategorií osobních údajů stanoví nařízení.[20]

4. Poskytnuté osobní údaje zvláštních kategorií jsou pokládány za důvěrné informace a v rámci jejich dalšího zpracování v rámci krajského úřadu se s nimi mohou seznamovat pouze oprávněné osoby,

[16] Článek 6 nařízení.
[17] Článek 7 nařízení.
[18] Článek 7 odst. 3 nařízení.
[19] Článek 9 odst. 2 nařízení.
[20] Článek 9 odst. 2 a 3 nařízení.

které tyto údaje potřebují pro plnění svých pracovních povinností. Za zabezpečení omezení přístupu k těmto údajům odpovídá vedoucí věcně příslušného odboru.

Čl. XII.
Oznamovací povinnost vůči veřejnosti

1. Oznamovací povinnosti vůči veřejnosti podléhá takové zpracování osobních údajů, které kraji (krajskému úřadu) ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona. Informace o zpracování osobních údajů je zveřejněna na oficiálních webových stránkách kraje.

2. Oznamovací povinnost vůči veřejnosti zajišťuje vedoucí odboru kancelář ředitelky krajského úřadu ve spolupráci s pověřencem na základě předaných informací od vedoucích věcně příslušných odborů.

Čl. XIII.
Znehodnocení osobních údajů

1. Zpracování osobních údajů je ukončeno:
   a) jakmile pomine účel, pro který byly údaje zpracovávány,
   b) na základě žádosti subjektu údajů v případě, že
      - kraj (krajský úřad) zpracovává jeho osobní údaje, přičemž zpracování je v rozporu s právem na ochranu soukromého a osobního života, nebo
      - jsou osobní údaje nepřesné s ohledem na účel jejich zpracování, nebo
      - odvolá svůj souhlas se zpracováním osobních údajů.

2. Osobní údaje, jejichž zpracování bylo ukončeno, musí být zlikvidovány s výjimkou:
   a) uchování osobních údajů pro účely archivnictví (lhůty uchování jsou stanoveny ve Skartačním plánu, který je součástí Spisového a skartačního řádu),
   b) uchování osobních údajů pro účely uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

Čl. XIV.
Předávání osobních údajů do zahraničí

1. K samotnému předání jinému správci musí mít správce stále právní důvod, jelikož i předání je jednou z činností zpracování osobních údajů.

2. K jakémukoli předání osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít pouze tehdy, splní-li správce a zpracovatel v závislosti na dalších ustanoveních tohoto nařízení stanovené podmínky uvedené v kapitole V. nařízení.[21]

[21] Článek 44 – 50 nařízení.

Čl. XV.
Smluvně zajištěný zpracovatel

Zpracovatelé, kterými jsou pověřené osoby dle čl. II. odst. 10 písm. b), mohou pro krajský úřad zpracovávat osobní údaje pouze v souladu s podmínkami zakotvenými ve smlouvě, která má vždy písemnou formu a náležitosti dle nařízení[22].

Čl. XVII.
Závěrečná ustanovení

1. Zrušuje se směrnice ředitelky č. SE 02/2012.

2. Tato směrnice ředitelky nabývá účinnosti dnem podpisu.

3. Tato směrnice ředitelky může být doplňována jednotlivými pokyny ředitelky krajského úřadu pro konkrétní oblasti.

Přílohy
Příloha č. 1 Přehled účelů zpracování osobních údajů
Příloha č. 2 Vzorový souhlas s použitím osobních údajů
Příloha č. 3 Záznamový list

V Karlových Varech dne 1. 10. 2018

Mgr. Martina Vránová, v.r.
ředitelka krajského úřadu

[22] Článek 28 nařízení.