Grant Thornton

An instinct for growth™

Zpracování systémové analýzy působnosti krajů z hlediska obecného nařízení o ochraně osobních údajů pro Česká republika – Ministerstvo vnitra

Závěrečná zpráva

Shrnutí

Systémová analýza působnosti krajů z hlediska obecného nařízení o ochraně osobních údajů byla zpracována na základě smlouvy č.j. MV-129479-1/LG-2017 uzavřené mezi Ministerstvem vnitra České republiky a Grant Thornton Advisory s.r.o.

Dne 25. května 2018 nabývá účinnosti 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). Nová právní úprava neznamená zlomový předěl v přístupu k ochraně osobních údajů. Nařízení však nad rámec dosavadní praxe v českém prostředí zpřesňuje a podrobněji popisuje některé požadavky a současně stanoví několik nových požadavků.

Systémová analýza byla provedena na vzorku 3 krajů a vztahuje se jak ke všem agendám v přenesené působnosti krajů, tak k základním (všem krajům společným) agendám v samostatné působnosti. Systémová analýza pokrývá také zákonem vymezené činnosti právnických osob zřizovaných kraji (v minimálním rozsahu vzorku obsahujícího školu a školské zařízení, zdravotnické zařízení, zařízení sociálních služeb, kulturní zařízení a oblast dopravní obslužnosti).

Tento dokument popisuje metodiku zpracování systémové analýzy, posouzení současného stavu a doporučení pro zjištěné nesoulady. Každá část systémové analýzy zohledňuje specifika krajů a právnických osob zřizovaných kraji tak, aby výstup byl pro kraje a právnické osoby zřizované kraji co nejvíce využitelný.

V rámci systémové analýzy bylo provedeno dotazníkové šetření na vzorku krajů a právnických osob zřizovaných kraji. Pro posouzení situace byla provedena analýza rizik v souladu s doporučeními GDPR. Na základě analýzy obdržených informací a výsledků analýzy rizik byly stanoveny nesoulady, a to v oblasti organizačně právní a v technické oblasti. Pro tyto nesoulady byl zpracován přehled doporučení, který zahrnuje základní aspekty dosažení požadované úrovně ochrany osobních údajů, a zároveň nastiňuje vhodný plán realizace těchto doporučení.

Systémová analýza se taktéž zabývá problematiku pověřence pro ochranu osobních údajů co do kvalifikačních požadavků, jeho podpory ze strany organizace a jeho základních úkolů. Dokument dále popisuje povinnost provádění posouzení vlivu na ochranu osobních údajů (DPIA) v případě, kdy je identifikováno vysoké riziko pro subjekt údajů.

Přehled zkratek a pojmů

Zkratka / pojem	Popis
MVČR (dále také „zadavatel“)	Česká republika – Ministerstvo vnitra
OÚ	Osobní údaj
COÚ	Citlivý osobní údaj - Zvláštní kategorie osobních údajů a osobní údaje týkající se rozsudků v trestních věcech a trestných činů
GAP analýza	Rozdílová analýza
SIEM	Security information and event. management, systém pro sběr a vyhodnocování bezpečnostních incidentů
SOC	Security operations center, bezpečnostní operační centrum
GDPR	General Data Protection Regulation, regulace EU 2017/679 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a volném pohybu těchto údajů
ISMS	Information security management systems, systém řízení bezpečnosti informaci dle rodiny ISO 27000
IS	Informační systém
SÚ	Subjekt údajů
DPIA	posouzení vlivu na ochranu osobních údajů
RIA	Hodnocení dopadů regulace (z anglického Regulatory Impact Assessment) je souborem kroků analyzujících očekávané dopady navrhovaných právních předpisů.

Obsah

1 Vymezení předmětu systémové analýzy

Systémová analýza byla provedena na vzorku 3 krajů vybraných zadavatelem a vztahuje se jak ke všem agendám v přenesené působnosti krajů, tak k základním (všem krajům společným) agendám v samostatné působnosti (se zaměřením na obecný rámec základních činností všech krajů v oblasti výkonu samostatné působnosti - poskytování dotací, dispozice majetkem, personální agenda, nakládání s osobními údaji o členech zastupitelstva kraje a členech iniciačních a poradních orgánů kraje apod.).

Systémová analýza pokrývá také zákonem vymezené činnosti právnických osob zřizovaných kraji (v minimálním rozsahu vzorku obsahujícího školu a školské zařízení, zdravotnické zařízení, zařízení sociálních služeb, kulturní zařízení a oblast dopravní obslužnosti).

Do vzorku 3 krajů byly vybrány:

- Moravskoslezský kraj,
- Karlovarský kraj,
- Středočeská kraj.

Pro účely posouzení právnických osob zřizovaných kraji byly vybráni následující zástupci:

- Škola a školské zařízení (Gymnázium Říčany, Dům dětí a mládeže Mělník),
- Zdravotnické zařízení (Zdravotnická záchranná služba Středočeského kraje, Dětské centrum Kladno),
- Zařízení sociálních služeb (Zařízení sociální intervence Kladno, Domov Laguna Psáry),
- Kulturní zařízení (Středočeská vědecká knihovna v Kladně),
- Oblast dopravní obslužnosti (Integrovaná doprava Středočeského kraje).

1.1 Kraje

V rámci analýzy krajů byly zpracovány následující agendy (oblasti zpracování OÚ / COÚ):

- Doprava,
- Školství, mládež, tělovýchova,
- ŽP a zemědělství,
- Územní plánování, stavební úřad,
- Kultura a památková péče,

- Regionální rozvoj a cestovní ruch,
- Kontrola,
- Kancelář hejtmana a vnějších vztahů,
- Podpora řízení,
- Kancelář ředitele úřadu,
- Legislativa a právo,
- Krajský živnostenský úřad,
- Sociální věci,
- Zdravotnictví,
- Investice a majetek,
- Finance,
- Bezpečnost a krizové řízení,
- Dotace a projekty,
- Interní audit.

1.2 Právnické osoby zřizované kraji

V rámci analýzy právnických osob zřizovaných kraji byly identifikovány následující agendy (oblasti zpracování OÚ / COÚ):

- Personálně-mzdová agenda (společné pro veškeré typy organizací),
- Úsek ekonomicko-provozní (společné pro veškeré typy organizací),
- Agenda pedagogiky (škola a školské zařízení),
- Poskytování zdravotních služeb (zdravotnické zařízení),
- Poskytování sociálních služeb (zařízení sociálních služeb),
- Knihovnické a informační služby (kulturní zařízení),
- Agenda dopravní obslužnosti (oblast dopravní obslužnosti).

1.3 Základní pojmy

- **Osobní údaj**. Veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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.
- **Citlivý údaj (zvláštní kategorie osobních údajů).** Osobní údaj, který vypovídá o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetický údaj nebo biometrický údaj jedinečně identifikující subjekt údajů a údaj o zdravotním stavu či o sexuálním životě nebo sexuální orientaci subjektu údajů.
- **Zpracování osobních údajů.** Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů,

jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

- **Subjekt údajů.** Fyzická osoba, k níž se osobní údaje vztahují a která je na základě těchto údajů identifikovaná nebo identifikovatelná.
- **Správce.** Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.
- **Zpracovatel.** Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

1.4 Dopady obecného nařízení o ochraně osobních údajů na kraje

Dne 25. května 2018 nabývá účinnosti[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), (dále jen „**Nařízení**“ nebo „**GDPR**“), které spolu se zákonem o zpracování osobních údajů nahradí dosavadní právní úpravu, tj. zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**zákon o ochraně osobních údajů**“).

Nová právní úprava neznamená zlomový předěl v přístupu k ochraně osobních údajů. Nařízení však nad rámec dosavadní praxe v českém prostředí zpřesňuje a podrobněji popisuje některé požadavky a současně stanoví několik nových požadavků, týkajících se zejména:

- povinností uložených správci a zpracovateli osobních údajů,
- práv subjektů, jejichž osobní údaje se zpracovávají (dále jen „**subjekt údajů**“).

Základní principy spojené se zpracováním osobních údajů, kterými je nutno se v současné době řídit se zásadně nemění, Nařízení však klade velký důraz na to, aby se smysl a účel těchto zásad promítl do všech jednotlivých procesů vykonávaných v rámci zpracování osobních údajů.

I přes deklarovanou právní kontinuitu v přístupu k ochraně osobních údajů, nelze odhlížet od toho, že nová právní úprava je mnohem podrobnější, než byla ta dosavadní.

Z novinek obsažených v Nařízení týkajících se krajů jako správců osobních údajů lze uvést povinnost správce vést záznamy o činnostech zpracování, povinnost jmenovat pověřence pro ochranu osobních údajů, povinnost ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů (dále jen „**Úřad**“ nebo „**ÚOOÚ**“); rozšíření práv subjektu údajů lze spatřovat v právu subjektu údajů na přenositelnost osobních údajů od jednoho správce ke druhému.

[1] V případě tohoto právního předpisu Nařízení hovoří o přímé použitelnosti, přičemž tento pojem lze v právním prostředí ČR ztotožnit s pojmem účinnosti právního předpisu.

1.4.1 Účel tohoto dokumentu

Tento dokument si klade za cíl seznámit osoby, které zpracovávají osobní údaje, v kontextu činností krajů,[2] s právní úpravou ochrany osobních údajů představovanou Nařízením.

Tento dokument, nechť je obecným interpretačním vodítkem při posouzení dopadů Nařízení na činnost krajů. Záměrem tohoto dokumentu není rozbor konkrétních situací, které s ohledem na šíři adresátů Nařízení lze velice těžko obsáhnout, ale stručný přehled jednotlivých dopadů GDPR na činnosti krajů. Tento dokument se tak věnuje výkladu budoucí právní úpravy způsobem, který by měl její aplikaci v prostředí krajů zjednodušit.

Tomuto záměru odpovídá i struktura dokumentu, přičemž v úvodní části je popsáno, o jakou právní úpravu se jedná, komu je dokument určen, na co je potřeba se v souvislosti s právní úpravou připravit a dále jsou zde též uvedeny zásady pro další nakládání s osobními údaji.

1.4.2 Pro koho je tento dokument určen?

Kraj může při zpracování osobních údajů vystupovat v roli správce, nebo zpracovatele osobních údajů. Kraj je správcem tehdy, když určuje účely a prostředky zpracování osobních údajů, případně když tento účel a prostředky ukládá zákon. Kraj je zpracovatelem, pokud zpracovává činnosti pro (jiného) správce, přičemž i tento proces může být definován přímo zákonem. Autor tohoto textu se domnívá, že v případě realizace činností v rámci výkonu přenesené působnosti budou kraje zásadně vystupovat v roli zpracovatele. Za zpracování osobních údajů je vždy primárně odpovědný správce (čl. 5 odst. 2 a čl. 24 odst. 1 Nařízení).

Kraje v rámci svých činností zajišťují plnění mnoha úkolů svěřených jim příslušnými právními předpisy,[3] mezi nejvýznamnější činnosti krajů patří např. plnění úkolů v oblasti:

- dopravy, kdy kraje jsou vlastníkem silnic II. a III. třídy, zřizovatelem příspěvkové organizace Krajské správy a údržby silnic, silničním správním úřadem a speciálním stavebním úřadem pro silnice I. třídy,
- sociálních služeb, kraje jako své příspěvkové organizace zřizují centra sociálních služeb, domovy seniorů, azylové domy, stacionáře a další poskytovatele sociálních služeb, krajský úřad vede registr poskytovatelů sociálních služeb, kraje zajišťují sociálně právní ochranu dětí,
- zdravotnictví, kraje zřizují a řídí krajské nemocnice, krajské úřady udělují oprávnění k poskytování zdravotních služeb, kraje jako své příspěvkové organizace zřizují zdravotnickou záchrannou službu a dětská centra,
- školství, kraje zřizují a řídí střední školy a vyšší odborné školy, mohou být zřizovatelem také mateřských, základních a základních uměleckých škol, zřizují domy dětí a mládeže, dětské domovy, pedagogicko-psychologické poradny,
- regionálního rozvoje, poskytují dotace z krajských fondů,

[2] Pro účely tohoto dokumentu bude pojem kraj vykládán v souladu s ustanovením § 1 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů.
[3] Srov. katalog činností krajů dostupný na http://www.mvcr.cz/clanek/katalog-cinnosti-obci.aspx

- kontroly a hospodaření, kraje přezkoumávají hospodaření obcí a dobrovolných svazků obcí, provádí finanční kontroly ve smyslu zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě v rozsahu stanoveném vnitřními předpisy kraje,
- bezpečnosti, kraje zřizují Bezpečnostní radu kraje, koordinují a koncepčně připravují řešení krizových situací,
- legislativy a správy, vydávají nařízení kraje, zajišťují činnosti volebního orgánu pro volbu prezidenta ČR a volby do Evropského parlamentu, parlamentu ČR, zastupitelstev krajů a obcí, vedou agendu veřejnoprávních smluv, vydávají osvědčení k zahájení veřejné sbírky,
- kultury, kraje jako své příspěvkové organizace zřizují regionální muzea, galerie, knihovny, poskytují dotační programy a granty pro podporu kultury v kraji,
- kraje zajišťují vedení registrů, evidencí a statistických přehledů z nejrůznějších oblastí svého správního obvodu.

S ohledem na výše uvedený demonstrativní přehled agendy krajů vyplývající z příslušných právních předpisů,[4] je nutné konstatovat, že tento výčet není zdaleka úplný, neboť kraje vystupují rovněž jako subjekty právních vztahů, např. jako objednatelé určitého plnění či jako zaměstnavatelé. Tento dokument je tak adresována všem osobám, které v rámci své činnosti přicházejí do styku s problematikou osobních údajů při vyřizování agendy krajů. Může se jednat např. o:

- členy zastupitelstva kraje, rady kraje, zvláštních orgánů kraje a jejich výborů a komisí,
- ředitele a vedoucí pracovníky příspěvkových organizacích,
- zaměstnance krajských úřadů a příspěvkových organizací,
- obchodní společnosti, v nichž má kraj svou majetkovou účast,
- správce sítě, jiné pracovníky IT a další.

Jako příklady zpracování osobních údajů fyzických osob v rámci vyřizování agendy krajů lze uvést zpracování osobních údajů týkajících se zaměstnanců krajského úřadu, příspěvkových organizací, studentů škol (jejich zákonných zástupců), pacientů krajských nemocnic, subjektů smluv, jichž jsou kraje smluvními stranami.

[4] Např. se jedná o zákon č. 129/2000 Sb., o krajích, zákon č. 365/2000 Sb., o informačních systémech veřejné správy, zákon č. 499/2004 Sb., o archivnictví a spisové službě, zákon č. 273/2001 Sb., o právech příslušníků národnostních menšin, zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu (zákon o ověřování), zákon č. 133/2000 Sb., o evidenci obyvatel, zákon č. 301/2000 Sb., o matrikách, jménu a příjmení, zákon č. 200/1990 Sb., o přestupcích, zákon č. 553/1991 Sb., o obecní policii, zákon č. 424/1991 Sb., o sdružování v politických stranách a v politických hnutích, zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky, zákon č. 111/1994 Sb., o silniční dopravě, zákon č. 13/1997 Sb., o pozemních komunikacích, zákon č. 20/1987 Sb., o státní památkové péči, zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon), zákon č. 248/2000 Sb., o podpoře regionálního rozvoje, zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), zákon č. 110/1998 Sb., o bezpečnosti České republiky.

1.4.3 Přehled jednotlivých dopadů Nařízení na kraje

Níže je uveden stručný přehled jednotlivých dopadů Nařízení na činnost krajů, který se zaměřuje především na oblasti, v nichž kraje budou muset přijmout určitá opatření, resp. se budou muset přizpůsobit požadavkům vyplývajícím z Nařízení.

1.4.3.1 Kraje musí provést kontrolu osobních údajů

Kraje musí zejména prověřit, zda osobní údaje fyzických osob zpracovávají na základě určitého legitimního účelu a dostatečného právního titulu dle čl. 6 Nařízení. Zpracování osobních údajů bude v řadě případů krajem prováděno zcela jistě z důvodu nezbytného pro splnění právní povinnosti (tedy zákonné povinnosti), relevantními však budou i jiné právní tituly – např. oprávněný zájem správce, plnění smlouvy či souhlas subjektu údajů.

Kraje musí dále prověřit, zda osobní údaje jsou zpracovávány v rozsahu, který je nezbytný ve vztahu k účelu, pro který jsou osobní údaje zpracovávány, tzn. zda je rozsah osobních údajů skutečně nezbytný pro výkon konkrétní činnosti (např. uvedení zaměstnání dětí osob umístěných do domova důchodců v žádosti o umístění osoby do domova důchodců nejspíše není nutným údajem, kterým domov důchodců coby příspěvková organizace zřízená krajem potřebuje v tomto smyslu disponovat).

Kraje musí zjistit, zda všechny takto zpracovávané osobní údaje jsou zpracovávány řádně a v souladu s právními předpisy. V této souvislosti např. vznikne též potřeba zkontrolovat dodavatelské smlouvy, které mají kraje nebo jejich příspěvkové organizace uzavřeny s poskytovateli informačních systémů či jiných IT služeb, v rámci, kterých jsou zpracovávány osobní údaje subjektů údajů; kontrola by měla být zaměřena zejména na způsoby zpracování osobních údajů, možnosti přístupu jednotlivých osob do systému, zabezpečení atd.[5]

1.4.3.2 Kraje musí provést kontrolu právních titulů zpracování

Kraj musí prověřit, na základě jakého právního titulu zpracovává osobní údaje, resp. zda má pro každou činnost zpracování stanoven právní titul zpracování. Nařízení uvádí výčet možných právních titulů v čl. 6 GDPR, resp. v čl. 9 GDPR v případě zpracování citlivých osobních údajů. Existence právního titulu je nezbytným předpokladem pro zpracování osobních údajů. Pokud správce nedisponuje právním titulem, nemůže osobní údaje zpracovávat.

V této souvislosti je potřeba rovněž provést revizi souhlasů doposud udělených ze strany subjektů údajů, tedy zda je souhlas v daném případě relevantním právním titulem pro zpracování (např. souhlas zaměstnance k použití jeho fotografie do příslušného identifikačního průkazu není odpovídajícím právním titulem, neboť v daném případě jsou osobní údaje zaměstnance zpracovávány na základě oprávněného zájmu správce). V případě, kdy souhlas bude odpovídajícím právním titulem, musí splňovat náležitosti dle Nařízení, především z hlediska požadavku na konkrétní rozsah zpracovávaných údajů (výčet), konkrétní účel a uvedení doby zpracování.

[5] Srov. článek 6 Nařízení.

Poskytované souhlasy by také měly být formulovány dostatečně konkrétně (např. „Souhlasím po dobu školního roku x/y se zveřejněním fotografií mého dítěte pořízených během akcí střední školy na webových stránkách školy, pokud nebude podobizna dítěte spojena s jeho jménem.“). Pokud znění souhlasu nebude vyhovovat požadavkům Nařízení, bude nutné, aby správce získal souhlas v podobě, která bude souladná s požadavky GDPR, jinak nesmí osobní údaje dále zpracovávat.

1.4.3.3 Kraje musí provést kontrolu uzavřených smluv

Kraje musí provést kontrolu smluv uzavřených se zpracovateli osobních údajů, na základě, nichž se zpracovávají osobní údaje, zejména se jedná o kontrolu rozsahu, účelu a doby zpracování. V případě smlouvy na provoz informačního systému externím dodavatelem je nutné zjistit, zda daný informační systém určitá instituce kraje vlastní, tedy k němu má zdrojové kódy a zpracovává jej sama, či data v něm obsažená spravuje třetí osoba (poskytovatel informačních služeb), která se stará, aby informační systém fungoval. S tím souvisí kontrola obsahu smlouvy, a to zejména co do podmínek přístupu jednotlivých třetích osob k osobním údajům vedeným v informačních systémech.

Smlouva se zpracovatelem musí splňovat náležitosti stanovené v čl. 28 odst. 3 Nařízení.

Je odpovědností smluvních stran (kraj a poskytovatel služeb), aby zajistily, že plnění smlouvy bude probíhat v souladu s Nařízením. Text smluv by měl odpovídat záměru předcházet případnému nezákonnému zpracování osobních údajů, a to včetně nastavení vhodných technických a organizačních opatření k zabezpečení ochrany osobních údajů dle požadavků Nařízení.

1.4.3.4 Kraje budou muset provést změnu smluv, které odporují Nařízení

Kraje budou muset provést změnu smluv, které odporují Nařízení, eventuálně uzavřít nové smlouvy s dodavateli, pokud se tak dosud nestalo, aby byly osobní údaje subjektu údajů chráněny před možným zneužitím.

1.4.3.5 Kraje budou muset jmenovat pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů musí splňovat požadavky dle článku 37 Nařízení. Pověřenec bude „odborným konzultantem“, který rozumí jak zpracovávání osobních údajů, tak chodu příslušné instituce, a který bude prakticky řešit situace, které při zpracovávání osobních údajů nastanou. Nařízení nestanoví přesně kvalifikační předpoklady pověřence, ale požaduje, aby se jednalo o osobu, která bude jmenována na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů. Nařízení ve svém článku 37 odst. 3 umožňuje, aby jeden pověřenec působil ve vícero veřejných subjektech.[6]

[6] Srov. článek 37 - 39 Nařízení.

1.4.3.6 Přijetí vnitřního předpisu o ochraně osobních údajů

Výsledkem všech výše uvedených kroků, jejichž provedením by mělo dojít k zamezení negativních dopadů souvisejících s Nařízením na činnost krajů, by mělo být vytvoření funkčního systému ochrany osobních údajů včetně jeho kontrolních mechanismů, aby se do budoucna zabránilo jakémukoliv potenciálnímu zneužití osobních údajů. Kraje by měly minimalizovat zpracovávání osobních údajů a snažit se o maximální pseudonymizaci[7] osobních údajů tam, kde je to možné a účelné. Výsledkem takového procesu může také být přijetí směrnice o ochraně osobních údajů, ve které se nastavený systém ochrany osobních údajů popíše včetně pravidel pro nakládání a další zpracovávání osobních údajů.[8]

1.4.4 Novinky v ochraně osobních údajů dle Nařízení

1.4.4.1 Přehled novinek

- zavedení institutu pověřence pro ochranu osobních údajů,[9]
- úprava postupu, jakým se může subjekt údajů obracet na správce či zpracovatele údajů, včetně povinnosti správce ve stanovené lhůtě žádosti vyhovět nebo informovat subjekt údajů o nepřijetí požadovaných opatření, spolu s informací o možnosti podat stížnost u dozorového úřadu či soudu v souladu s článkem 12 odst. 4 Nařízení,[10]
- výslovná úprava tzv. práva být zapomenut v článku 17 odst. 2 Nařízení znamená zakotvení povinnosti pro správce osobních údajů, který osobní údaje zveřejnil a je povinen je vymazat, informovat všechny další správce, kteří tyto osobní údaje zpracovávají, že subjekt údajů žádá o výmaz veškerých odkazů na tyto osobní údaje, jejich kopie či replikace,[11]
- rozšíření důvodů, pro které je možné požadovat po správci omezení zpracování údajů dle článku 18 Nařízení,[12] což nemusí znamenat, že ze strany subjektu údajů došlo k úplnému zákazu zpracovávání,[13]
- právo na přenositelnost údajů dle článku 20 Nařízení v případě zpracovávání osobních údajů na základě souhlasu či za účelem splnění smlouvy, pokud se zároveň provádí zpracování automatizovaně, má subjekt údajů právo získat osobní údaje, které se ho týkají ve

---

[7] Dle článku 4 odst. 5 GDPR se „pseudonymizací" rozumí: „*zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné osobě.*"

[8] Srov. článek 32 Nařízení.

[9] Viz ustanovení článků 37- 39 Nařízení.

[10] Např. formou interního předpisu přijatého vedením příslušné instituce a zveřejněného na internetových stránkách, úřední desce či jiným způsobem; v této souvislosti upozorňujeme, že žádný vnitřní předpis nemůže omezit právo subjektu údajů žádat informace od správce nebo zpracovatele o jeho osobních údajích, stejně tak vnitřní předpis přijatý správcem nebo zpracovatelem nezavazuje subjekt údajů, ten se svého práva může domáhat pouze na základě Nařízení bez omezení.

[11] Srov. článek 17 Nařízení.

[12] Dříve tzv. blokace dle ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů.

[13] Srov. článek 18 Nařízení.

strukturovaném, běžně používaném a strojově čitelném formátu, případně může správce požádat, aby jeho osobní údaje byly takto poskytnuty správci dalšímu,[14]

- právo vznést námitku proti zpracování osobních údajů v případě, že dochází ke zpracování údajů nezbytnému pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, případně je-li to nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany dle článku 21 Nařízení např. zpracování osobních údajů uchazeče o zaměstnání při výběrovém řízení,[15]
- princip záměrné a standardní ochrany osobních údajů dle čl. 25 Nařízení,
- zpřísnění a zpřesnění požadavků k úpravě smlouvy o zpracování osobních údajů dle čl. 28 odst. 3 Nařízení,
- povinnost vést záznamy o činnostech zpracování v rozsahu a za podmínek upravených v článku 30 Nařízení,
- ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a oznamování případů porušení zabezpečení osobních údajů subjektu údajů za podmínek uvedených v článcích 33 a 34 Nařízení,
- zpřísnění podmínek předávání osobních údajů do třetích zemí nebo mezinárodním organizacím dle článku 44 a násl. Nařízení. Předávání osobních údajů do třetí země, kterou se rozumí stát, jenž není členem Evropské unie, se bude moci uskutečnit předně, pokud Evropská komise rozhodla, že bude zajištěna odpovídající úroveň ochrany a takové rozhodnutí uveřejnila v Úředním věstníku Evropské unie a na svých stránkách, případně za splnění podmínek článku 46 Nařízení.

1.4.4.2 Instituty, se kterými se kraje mohou při ochraně osobních údajů setkat

- žádosti subjektů údajů uplatňujících práva na přístup k osobním údajům,[16] opravu[17] či výmaz osobních údajů,[18] případně omezení jejich zpracování,[19] anebo týkající se realizace práva na přenositelnost údajů,[20]
- uplatnění práva subjektu údajů na informace dle článku 13 a násl. Nařízení,
- uplatnění práva subjektu údajů podat námitku proti zpracování osobních údajů dle článku 21 Nařízení.

[14] Srov. článek 20 Nařízení.
[15] Srov. článek 21 Nařízení.
[16] Srov. článek 15 Nařízení.
[17] Srov. článek 16 Nařízení.
[18] Srov. článek 17 Nařízení.
[19] Srov. článek 18 Nařízení.
[20] Srov. článek 20 Nařízení.

1.4.4.3 Záměrná a standardní ochrana osobních údajů

Nařízení v čl. 25 odst. 1 zakotvuje koncept záměrné ochrany osobních údajů (tzv. „data protection by design") a v čl. 25 odst. 2 požadavek standardní ochrany osobních údajů (tzv. „data protection by default"). Jedná se o významné prvky principu odpovědnosti upraveného v čl. 24 GDPR, podle něhož je správce povinen zavést vhodná technická a organizační opatření, aby 1) zajistil, že při zpracování osobních údajů postupuje v souladu s Nařízením, a zároveň 2) aby byl schopen tento soulad postupů s Nařízením doložit. Při zavedení vhodných technických a organizačních opatření přitom správce musí zohlednit povahu, rozsah, kontext a účely zpracování a zejména analyzovat rizika, s nimiž je zpracování spojeno, pro práva a svobody fyzických osob (čl. 24 odst. 1 GDPR). Jedná se zejména o nastavení vhodných koncepcí v oblasti ochrany osobních údajů (čl. 24 odst. 2 GDPR). Správce by proto měl přijmout interní předpisy na ochranu osobních údajů, případně pokud tyto předpisy a případně další interní předpisy, které se zpracování osobních údajů týkají, již přijal, měl by provést jejich revizi. Účelem těchto předpisů je stanovení jednoznačných a srozumitelných pokynů zaměstnancům správce, kteří se podílejí na činnostech zpracování osobních údajů.[21] S tím souvisí provádění řádné dokumentace postupů správce při zpracování osobních údajů, která bude dokladovat plnění jednotlivých povinností správce a na základě níž správce bude schopen prokazovat soulad jeho postupů s GDPR. Princip odpovědnosti správce dle čl. 24 odst. 1 GDPR tak spočívá ve vytvoření komplexního systému opatření s cílem zajistit soulad postupů správce s Nařízením, který bude třeba v případě změny okolností (vnitřních i vnějších) revidovat a aktualizovat.[22]

Z článku 24 odst. 1 Nařízení dále plyne, že správce bude muset prokázat i zavedení opatření přijatých k zajištění záměrné a standardní ochrany osobních údajů.

Koncept záměrné ochrany osobních údajů ukládá správci již při určování prostředků zpracování zavést vhodná technická a organizační opatření, a to za účelem provedení zásad ochrany osobních údajů a začlenění nezbytných záruk do zpracování tak, aby správce plnil požadavky Nařízení a ochránil práva subjektu údajů. Správce tato opatření zvolí na základě uvážení stavu techniky, nákladů na provedení opatření, povahy, rozsahu, kontextu a účelů zpracování a také pravděpodobnosti a závažnosti rizik pro práva a svobody fyzických osob, jež zpracování představuje. Smyslem této úpravy je, aby správce ještě před samotným zpracováním osobních údajů přistupoval k volbě prostředků zpracování s ohledem na práva a svobody osob a za účelem toho, aby dostál svým povinnostem v oblasti ochrany osobních údajů. Nařízení uvádí jako příklad provádění pseudonymizace, relevantní jsou též ostatní bezpečnostní opatření uvedená v čl. 32 odst. 1 GDPR.

Koncept standardní ochrany osobních údajů ukládá správci povinnost přijmout vhodná technická a organizační opatření k zajištění toho, aby standardně byly zpracovávány pouze takové osobní údaje,

---

[21] Uvedené souvisí také se zněním čl. 29 GDPR, podle něhož „*zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu.*"

[22] Viz NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR/Obecné nařízení o ochraně osobních údajů: praktický komentář. 1. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3.

které budou pro konkrétní účel nezbytné, a to jak z hlediska množství shromážděných údajů, tak rozsahu jejich zpracování, doby uložení a jejich dostupnosti. Jedná se o projev zásady minimalizace údajů a zásady omezení uložení upravené v čl. 5 odst. 1 písm. c) a e) GDPR, přičemž předmětné ustanovení ukládá správci přijmout konkrétní opatření za účelem provedení těchto zásad. Účelem těchto opatření je dle Nařízení zejména zajistit, aby osobní údaje nebyly standardně zpřístupňovány neomezenému počtu fyzických osob.

K výše uvedenému je vhodné doplnit, že dle recitálu 78 Nařízení by zásady záměrné a standardní ochrany měly být správcem zohledněny rovněž v souvislosti s veřejnými zakázkami.

1.4.5 Základní doporučení k implementaci Nařízení

Pro zmírnění dopadů Nařízení na kraje, lze navrhnout, aby se kraje řídili při implementaci Nařízení níže definovanými doporučeními.

Uvést do 25. května 2018, tj. dne nabytí účinnosti Nařízení, všechny postupy a způsoby zpracovávání osobních údajů a také všechny smlouvy a jiné právní dokumenty **do souladu s požadavky Nařízení.**

Při zpracování osobních údajů vždy dodržovat zásady zpracování dle čl. 5 Nařízení. (zásada zákonnosti, korektnosti a transparentnosti, zásada účelového omezení, minimalizace údajů, přesnosti, omezení uložení a zásada integrity a důvěrnosti)

- Např. zvážit, ve kterých případech jsou konkrétní osobní údaje opravdu třeba, kdy je nutné znát např. rodná čísla uchazečů o zaměstnání.

Prověřit, na základě, jakých právních titulů provádí správce zpracování osobních údajů.

- Např. zpracování nezbytné pro plnění právní povinnosti nebo pro splnění smlouvy, zpracování pro ochranu oprávněných zájmů nebo ve veřejném zájmu, na základě souhlasu se zpracováním osobních údajů.

Vyžadovat souhlas subjektu údajů jen v případech, kdy pro daný účel zpracování nelze využít jiný právní titul ke zpracování osobních údajů.

- Souhlas může subjekt údajů kdykoliv odvolat. Souhlas musí být svobodný a nelze jeho udělením podmiňovat mimo jiné plnění smlouvy – nelze doporučit spojovat podpis souhlasu se zpracováním konkrétních osobních údajů, za konkrétním účelem a na předem určenou dobu s podpisem jiného dokumentu, např. seznámení se s interní směrnicí zaměstnavatele, školním řádem.

Poskytovat informace subjektům údajů.

- Informace a poučení o nezbytnosti a potřebě zpracovávat osobní údaje je v případě, že osobní údaje byly získány přímo od subjektů údajů, nutné sdělit subjektům údajů v okamžiku tohoto získání, a to při splnění požadavků k obsahu a formě dle čl. 12 až 14 Nařízení.

Provést kontrolu uzavřených smluv.

- Kraje musí provést kontrolu smluv uzavřených se zpracovateli osobních údajů, na základě, nichž se zpracovávají osobní údaje, zejména se jedná o kontrolu rozsahu, účelu a doby zpracování.

Revidovat vnitřní předpisy a mechanismy v oblasti ochrany osobních údajů a vést řádnou dokumentaci o zpracování osobních údajů.

- Nařízení je založeno na proaktivním přístupu správce k zajištění ochrany osobních údajů, a to nejen za účelem dodržování povinností, které Nařízení správci ukládá, ale též z důvodu, že správce musí být schopen doložit, že jeho postupy jsou souladné s Nařízením. Uvedené je projevem zásady odpovědnosti správce za dodržování GDPR (čl. 5 odst. 2, čl. 24 odst. 1 GDPR), z níž vychází koncept záměrné a standardní ochrany osobních údajů (čl. 25 odst. 1 a 2 GDPR).

Upravit vnitřní procesy tak, aby subjekt údajů mohl uplatnit svá práva podle čl. 15 až 22 Nařízení.

- Např. prostřednictvím vnitřního předpisu přijmout vhodná technická a organizační opatření.

2 Metodika zpracování systémové analýzy

Cílem systémové analýzy působnosti krajů z hlediska obecného nařízení o ochraně osobních údajů je identifikovat aktuální úroveň naplnění Nařízení pro kraje i právnické osoby zřizované kraji. Systémová analýza má sloužit jako základní popis zpracování osobních údajů v informačních systémech v kontextu činnosti krajů a zhodnotit, zda stávající činnosti krajů jsou či nejsou v souladu s obecným nařízením o ochraně osobních údajů. Dále pak je cílem zhodnotit typická rizika zpracování na daném vzorku dat a navrhnout opatření k nápravě v případě, kdy stávající činnost kraje je nesouladná s obecným nařízením o ochraně osobních údajů.

Tato analýza byla realizována ve 2 etapách. První etapou bylo posouzení souladu organizací s Nařízením. Druhá etapa navrhuje doporučení, jejichž realizace je doporučena pro naplnění souladu s GDPR.

V rámci první etapy byly rozeslány 3 typy dotazníků na společnosti uvedené v rámci Vymezení předmětu systémové analýzy:

- Dotazník Quick Check, který vyplňuje zpravidla zástupce bezpečnosti ve spolupráci s IT. Za danou organizaci je vyplněn pouze jeden dotazník. Tento dotazník slouží pro zpracování souhrnné analýzy připravenosti.
- Dotazník Přehled systémů, který vyplňuje zpravidla zástupce IT a techničtí zástupci aplikací (garant/vlastník aplikace). Za každou organizaci je vyplněn pouze jeden dotazník. Tento dotazník slouží pro zjištění všech informačních systémů, které obsahují OÚ/COÚ, a jejich bezpečnostních parametrů.
- Dotazník organizační a právní, který vyplňuje zpravidla zástupce za oddělení nebo danou agendu, je potřeba zpracovat pro každou agendu v rámci dané organizace (tj. krajského úřadu nebo příspěvkové organizace) zvlášť, a to jak v rámci výkonu samostatné působnosti (tj. druhý list dotazníku), tak v rámci výkonu přenesené působnosti (tj. třetí list dotazníku). Tento dotazník slouží jako podklad organizačního, procesního a právního posouzení.

Dotazy v jednotlivých dotaznících směřovaly též ke zjištění toho, zda a jaká organizační a technická opatření mají jednotlivé organizace zavedeny, na jaké úrovni a jaké je jejich uplatnění v praxi organizace v rámci výkonu činností ze strany pověřených osob (zaměstnanců).

Obdržené informace v rámci podkladových dokumentů a obdržených dotazníků nebyly dále zpracovatelem této analýzy ověřovány a byly považovány za pravdivé a popisující skutečnost.

2.1 Souhrnná analýza připravenosti

Pro zjištění základní připravenosti jednotlivých organizací na GDPR byl využit dotazník Quick Check, který na základě sady otázek a výběru z odpovědí posuzuje, jaká je míra rizika pro SÚ při zpracování OÚ/COÚ a jaká je míra organizačních a technických opatření. Tato míra rizika a opatření označuje „připravenost" organizace na GDPR a je porovnána s referenčními (doporučovanými) hodnotami, na stupnici 0 – 5 (0 nejnižší, 5 nejvyšší).

Procesy a opatření ochrany dat jsou hodnoceny v následujících oblastech (v závorce je uvedena referenční hodnota):

- Strategie a manuál k ochraně osobních údajů (3),
- Směrnice pro zaměstnance (3),
- Odpovědnosti ve společnosti (3),
- Činnosti zpracování (4),
- Zpracovávané údaje (3),
- Klasifikace dat (3),
- Infrastruktura/přenos dat/tok dat (3),
- Transparentnost a informace k poskytnutí (4),
- Analýza rizika (4),
- Integrace procesu (4),
- Procesy ochrany dat (3),
- Porušení ochrany dat (4),
- Zpracovatelé (3),
- Vědomí a trénink (4),
- Audit a kontinuální zlepšování (3).

Opatření informační bezpečnosti jsou hodnocena v následujících oblastech (v závorce je uvedena referenční hodnota):

- Obecné nároky na ochranná opatření (3),
- Bezpečnost osobní a bezpečnost prostředí (3),
- Kontrola přístupu (3),
- Bezpečnost sítě (3),
- Dostupnost (3),
- Bezpečnostní a nouzová opatření (3),
- Integrita (3),
- Odolnost (3),
- Bezpečnost komunikace (3),
- Šifrování (3),
- Logování (3).

Podkladem pro provedení analýzy byly informace získané vyplněním připravených formulářů (dotazníků). Respondenty byly vlastníci informací nebo garanti informačních systémů, zástupce bezpečnosti, případně další kompetentní osoby.

Výstup je rozdělen podle jednotlivých typů organizací, tedy na:

- Kraje,
- Škola a školské zařízení,
- Zdravotnické zařízení,
- Zařízení sociálních služeb,
- Kulturní zařízení,
- Oblast dopravní obslužnosti.

2.2 Organizační, procesní a právní posouzení

Organizační, procesní a právní posouzení vycházelo z metody dotazníkového šetření, na základě, které byl proveden sběr vstupních informací, které jsou nezbytné pro zpracování a vyhodnocení této části analýzy. Dotazy byly formulovány v kontextu znění Nařízení, účelem tedy bylo zjištění připravenosti organizace z hlediska požadavků stanovených v GDPR. Vzorový dotazník je umístěný v Příloha 10 – Dotazník právní. Dotazníky byly vyplněny dle jednotlivých agend členěných v rámci kraje či právnické osoby zřizované krajem, a to zástupci zvolenými v rámci krajského úřadu, resp. právnické osoby zřizované krajem. Dotazníky určené krajům byly dále děleny na samostatnou a přenesenou působnost. Cílem použité metody bylo zjištění aktuálního stavu zpracování osobních údajů v rámci činnosti krajského úřadu, resp. právnické osoby zřizované krajem, tedy zejm. získání přehledu o agendách, vykonávaných činnostech, při nichž dochází ke zpracování osobních údajů, rozsahu zpracovávaných osobních údajů a způsobu jejich uložení.

V rámci prvotní fáze vyhodnocování dotazníků byla posuzována úplnost poskytnutých odpovědí. V případě, že některé dotazy nebyly zcela zodpovězeny, byl dotazník vrácen s žádostí o doplnění konkrétních informací, které byly v žádosti specifikovány.

Dotazník_právní.xlsx obsahuje dotazy vztahující se zejména k těmto položkám:

- Činnosti, při nichž dochází ke zpracování osobních údajů,
- Role a odpovědnost osob podílejících se na zpracování,
- Kategorie a rozsah zpracovávaných osobních údajů,
- Kategorie subjektů údajů,
- Účel zpracování osobních údajů,
- Právní titul ke zpracování osobních údajů,
- Doba zpracování osobních údajů,
- Doba uložení osobních údajů,
- Plnění informační povinnosti vůči subjektu údajů,
- Kategorie příjemců včetně příjemců mimo EU,
- Využití zpracovatele osobních údajů,

- Úložiště dat ve fyzické a elektronické podobě,
- Uplatňování práv ze strany subjektů údajů,
- Způsob kontroly zpracování osobních údajů,
- Porušení zabezpečení osobních údajů.

2.2.1 Přehled zpracovávaných osobních údajů

Na základě poskytnutých informací v rámci dotazníkového šetření byl zpracován přehled činností, při nichž dochází ke zpracování osobních údajů dle jednotlivých agend modelového kraje a typu právnické osoby zřizované krajem (viz příloha č. 1 a příloha č. 2). Tento dokument nepředstavuje úplný výčet vykonávaných činností, při kterých dochází ke zpracování osobních údajů ani úplný rozsah zpracovávaných osobních údajů. Účelem dokumentu je především zjištění míry povědomí osob podílejících se na zpracování o požadavcích na ochranu osobních údajů a o postupech při práci s osobními údaji.

2.2.2 Přehled právních titulů

Na základě poskytnutých informací v rámci dotazníkového šetření byly ve vztahu k vykonávaným činnostem, při nichž dochází ke zpracování osobních údajů, určeny právní tituly ke zpracování osobních údajů a relevantní právní úprava (viz příloha č. 7 a příloha č. 8).

2.2.3 Přehled nesouladů

V rámci další fáze vyhodnocování dotazníků bylo přistoupeno k posouzení souladu procesů, během nichž dochází ke zpracování osobních údajů s požadavky, které vycházejí z GDPR.

Ke zpracování analýzy byla vyžádána relevantní dokumentace. Analýze v kontextu posouzení souladu procesů byly podrobeny zejména tyto interní předpisy a další dokumenty:

- Organizační řád,
- Pracovní řád,
- Spisový a skartační řád,
- Směrnice o ochraně osobních údajů,
- Směrnice pro evidenci zpracování osobních údajů,
- Směrnice pro ukládání dat,
- Politika bezpečnosti informací,
- Řád upravující některá vnitřní pravidla,
- Provozní řád,
- Směrnice pro personální práci,
- Vzorová pracovní smlouva,
- Vzorová dohoda o provedení práce,
- Vzorová dohoda o provedení pracovní činnosti,
- Vzorová smlouva o dílo,

- Vzorová kupní smlouva,
- Osobní dotazník,
- Dotazník člena zastupitelstva kraje,
- Souhlas zaměstnance se shromažďováním, zpracováváním a archivováním jeho osobních údajů v oblasti agendy personální, mzdové, daňové, sociálního a zdravotního pojištění,
- Souhlas zaměstnance s využitím osobních údajů pro účely vystavení pracovní smlouvy a jejích změn; pro účely zveřejnění ve vnitřním telefonním seznamu, pro účely zveřejnění na internetových stránkách krajského úřadu a pro účely zhotovení služebních průkazů zaměstnanců; pro účel přihlášení stravovacích karet u provozovatele závodního stravování; pro účely vystavení certifikátu, osvědčení o absolvování kursu, semináře, školení nebo zkoušky; pro účely poskytování preventivní zdravotní péče a cestovního pojištění do zahraničí,
- Vzorová smlouva o podnájmu nebytových prostor (Škola a školské zařízení),
- Vzorová smlouva o poskytnutí služeb (Škola a školské zařízení),
- Vnitřní řád (Škola a školské zařízení),
- Knihovní řád (Kulturní zařízení).

Posouzení procesů, během nichž dochází ke zpracování osobních údajů, včetně posouzení stávajících organizačních opatření, bylo prováděno s cílem určit vhodná organizační opatření, která je nezbytné zavést pro zajištění plného souladu hodnoceného procesu s GDPR. V rámci analýzy byla provedena identifikace nesouladu procesu či konkrétního postupu s požadavky vyplývajícími z jednotlivých článků GDPR. V rámci posuzování souladu bylo přihlíženo zejména k zásadám zpracování osobních údajů dle čl. 5 GDPR, tj. zásady zákonnosti, korektnosti a transparentnosti, zásady účelového omezení, zásady minimalizace údajů, zásady přesnosti, zásady omezení uložení, zásady integrity a důvěrnosti a zásady odpovědnosti.

Vzhledem ke skutečnosti, že systémová analýza byla provedena na vzorku 3 krajů a vzorku právnických osob zřizovaných kraji vybraných zadavatelem, výstup analýzy zahrnuje výčet veškerých identifikovaných nesouladů podle dotčených agend, tj. i v případě, že nesoulad byl identifikován pouze v rámci jednoho kraje či jednoho zástupce typu právnické osoby zřizované kraji.

Následně na základě identifikovaných nesouladů byla navržena vhodná organizační opatření. Tato opatření jsou uvedena v obecné rovině a je na příslušné organizaci, jaké zvolí nástroje, technologie a postupy pro realizaci doporučení k dosažení souladu s GDPR. Pro účely zavedení doporučení do praxe byla stanovena prioritizace dle níže uvedených stupňů (viz příloha č. 5 a příloha č. 6).

Stupeň	Hodnota	
1	Vysoká	Zavedení opatření je nezbytné. Nepřijetí opatření může vést k neakceptovatelnému porušení požadavků GDPR na zpracování osobních údajů. Porušení zákonných povinností bude mít vliv na fungování organizace jako celku.
2	Střední	Zavedení opatření je nezbytné. Nepřijetí opatření může vést k neakceptovatelnému porušení požadavků GDPR na zpracování osobních

		údajů. Porušení zákonných povinností nebude mít vliv na fungování organizace jako celku.

2.3 Přehled systémů, rizika

Na základě vyplnění dotazníku Přehled systémů business vlastníky a IT vlastníky, který je uveden v Příloha 3 – Přehled systémů (Kraje) a Příloha 4 – Přehled systémů (Právnické osoby zřizované kraji) list „Dotazník přehled systémů" byly získány informace o současném stavu systémů. Aby bylo možné zhodnotit soulad technických opatření v systémech a GDPR, byly otázky v Přehledu systémů voleny s ohledem na oddíl 2, článek 32 GDPR.

Na základě obdržených informací, byl identifikován současný stav technických opatření. Nevyplněné hodnoty (N/A) byly posuzovány jako nesplněné, tedy jako odpověď „NE". Celková analýza jednotlivých typů systémů je uvedena v kapitole 3.4. Systémy, které neobsahují OU, nejsou hodnoceny.

Soulad dostupných technických opatření v systémech vychází z odpovědí uvedených pro jednotlivé systémy a porovnává počet odpovědi „ANO" (soulad) vůči odpovědi „NE" (nesoulad) pro 16 parametrů.

Dotazník obsahuje:

- přehled systémů,
- přehled typů systémů,
- míru technických opatření,
- dopady na SÚ,
- rizika,
- IT opatření.

Výstup je rozdělen do dvou skupin na kraje a právnické osoby zřizované kraji.

2.3.1 Dotazník přehled systémů

Dotazník přehled systémů slouží jako přehled všech identifikovaných informačních systémů v organizaci. Tento dotazník byl zaslán k vyplnění jednotlivým organizacím, kde ho zpravidla vyplnil zástupce IT a techničtí zástupci aplikací (garant/vlastník aplikace). Za danou organizaci byl vyplněn jeden kompletní dotazník. Dotazník obsahuje základní údaje o systému a přehled 16-ti bezpečnostních parametrů, které souvisí s ochranou osobních údajů v daném systému (článek 32 Nařízení):

1. Zavedení pseudonymizace OU/COU.
2. Zavedení šifrování.
3. Zavedení přenosu dat výhradně šifrovanou komunikací, a to jak vně, tak i uvnitř společnosti.

4. Zavedení řízeného přístupu (přístupová práva uživatelů) k danému rozsahu OU nezbytných pro danou roli.
5. Zavedení auditních záznamů (logů) umožní odhalit chování uživatelů v systému a jejich přistupování k OU.
6. Zavedení dvoufaktorového ověření, které zajistí ověření identity uživatele 2 nezávislými způsoby.
7. Napojení na SIEM/SOC automatizuje identifikaci incidentů na základě sledování logů.
8. Nastavení řízené síťové komunikace.
9. Zvýšení dostupnosti systému prostřednictvím redundance/replikace (HA).
10. Zajištění pravidelného zálohování systému.
11. Zavedení disaster recovery plánu.
12. Zavedení plánu zálohování.
13. Zavedení pravidelného testování obnovy ze zálohy.
14. Zavedení pravidelného vyhodnocování incidentů.
15. Zavedení pravidelného testování DR scénáře.
16. Zavedení pravidelného testování zranitelností.

2.3.2 Přehled typů systémů

Přehled typů systémů představuje shrnutí bezpečnostních parametrů pro jednotlivé typy informačních systémů. Systémy získané v dotazníku přehled systémů od všech organizací byly rozděleny do skupin dle jejich funkcionalit do následujících skupin:

- spisová služba – systémy související s vykonáváním spisové služby
- ekonomický systém – personalistika, evidence majetku, účetnictví,…
- agendové IS a evidence[23]
- datový sklad
- docházkový systém
- dotace
- service desk – help desk
- webové portály – portály organizace, intranet, elektronická úřední deska,…
- krajské digitální úložiště
- technické – Active Directory, integrační sběrnice, identity management, zálohování,…
- kancelářský sw – Office,…
- kamerové systémy
- ostatní – systémy nespadající do jiných kategorií
- síťové disky

[23] Skupinu agendové IS a evidence představuje největší počet systémů pracující s OÚ. Tyto systémy jsou na základě dostupných podkladů zabezpečeny v průměru na stejné úrovni, proto jsou pro lepší přehlednost sloučeny do jedné skupiny.

- není k dispozici – v případě, kdy nebylo z dostupných informací zřejmé, o jaký systém se jedná, ale bylo uvedeno, že obsahuje OÚ anebo COÚ (vychází z dotazník právní).

Tyto typy informačních systémů byly vyhodnoceny z hlediska míry bezpečnosti jako průměr počtu odpovědí „ANO“ (odpovídá hodnotě 1) vůči odpovědím „NE“ (odpovídá hodnotě 0) všech systémů v dané kategorii, pro jednotlivé bezpečnostní parametry.

Získaný přehled výsledku bezpečnostních parametrů pro jednotlivé typy informačních systémů slouží pro posouzení míry technických opatření.

2.3.3 Míra technických opatření

Míra technických opatření určuje poměr mezi pravděpodobností IT hrozby vůči úrovni technických opatření. Jednotlivá opatření mají různou váhu daného technického opatření (1 – 3, přičemž 1 nízká váha, 2 střední váha, 3 vysoká váha bezpečnostního parametru). V případě, kdy je bezpečnostní parametr uveden jako splněný (hodnota = 1 viz kapitola Přehled typů systémů), je vynásoben hodnotou váhy, pokud je parametr pro daný typ systému nesplněn, je hodnota 0.

Výsledná Úroveň technických opatření pro daný typ systémů je odstupňována podle poměru mezi získaným hodnocením a maximem sumy všech vah jednotlivých bezpečnostních parametrů, tedy:

- hodnota 1 je v případě, kdy suma hodnocení daného typu systému je <= 2/6 sumy maximální hodnoty váhy
- hodnota 1,5 je v případě, kdy suma hodnocení daného typu systému je <= 3/6 sumy maximální hodnoty váhy
- hodnota 2 je v případě, kdy suma hodnocení daného typu systému je <= 4/6 sumy maximální hodnoty váhy
- hodnota 2,5 je v případě, kdy suma hodnocení daného typu systému je <= 5/6 sumy maximální hodnoty váhy
- hodnota 3 je v případě, kdy suma hodnocení daného typu systému je > 5/6 sumy maximální hodnoty váhy

Výsledná Pravděpodobnost hrozby je určena opačně k Úrovni technických opatření na stupnici 1 – 3, přičemž 1 znamená nízká, 2 střední, 3 vysoká. Např.: pokud je úroveň technických opatření 1, tak pravděpodobnost IT hrozby je 3.

2.3.4 Dopady na SÚ

Přehled dopadů na SÚ mapuje jednotlivé agendy, v nich jsou využívané typy systémů (mapování vychází z jednotlivých právních dotazníků – Dotazník právní) a typy OÚ a COÚ včetně rozsahu zpracování.

Výsledná Úroveň dopadu na SÚ je na stupnici 1 – 5 (1 nízká, 5 vysoká) uvedena jako maximální možná úroveň dopadu na SÚ na základě zjištěných skutečností vyplývajících z právních dotazníků.

2.3.5 Rizika

Výsledné riziko je uvedeno pro každou agentu a IS, ve kterém je daná agenda zpracována. Výsledné riziko je součin Pravděpodobnosti IT hrozby a Úrovně dopadu na SÚ. Výše rizika je na stupnici 1 – 15:

- nízké riziko 1,0 – 4,9
- střední riziko 5,0 – 7,9
- významné 8,0 – 11,9
- vysoké 12,0 – 15 (nutné provést posouzení vlivu na ochranu osobních údajů – DPIA, viz kapitola 4.3)

2.3.6 IT opatření

Popis přínosů jednotlivých bezpečnostních opatření:

1. Zavedení pseudonymizace OU/COU. Jedná se o proces skrytí identity subjektu údajů, který je pomocí příslušného klíče vratný. Například nahrazením jména číslem a v oddělené tabulce (databázi) držet číselník se jmény. Zjednoduší řízení přístupu konkrétních uživatelských rolí ke konkrétnímu výseku OU, které daná role potřebuje ke své práci (pokud daná role OU nepotřebuje a stačí jí pouze statistické údaje).

2. Zavedení šifrování. Zvýší úroveň zabezpečení systému proti neoprávněnému použití dat v případě odcizení databáze, která bude nečitelná. Ve formě elektronických dat lze šifrovat přenosovou vrstvu pro přenos dat, softwarovou vrstvu uložení dat a hardwarovou vrstvu úložiště, na kterém se data nacházejí.

3. Zavedení přenosu dat výhradně šifrovanou komunikací, a to jak vně, tak i uvnitř společnosti. Zamezení odcizení údajů pomocí odposlouchávání komunikace.

4. Zavedení řízeného přístupu (přístupová práva uživatelů) k danému rozsahu OU nezbytných pro danou roli. Omezení pravděpodobnosti neoprávněného přístupu dané role k OU a zejména získání celého obrazu OU danou rolí.

5. Zavedení auditních záznamů (logů) umožní odhalit chování uživatelů v systému a jejich přistupování k OU. Nezbytné při vyšetřování zneužití OU (reporting ÚOOÚ).

6. Zavedení dvoufaktorového ověření, které zajistí ověření identity uživatele 2 nezávislými způsoby. Snižuje možnost zneužití hesla.

7. Napojení na SIEM/SOC automatizuje identifikaci incidentů na základě sledování logů. Nezbytné při vyšetřování zneužití OU (reporting ÚOOÚ).

8. Nastavení řízené síťové komunikace. Řízení síťové komunikace snižuje riziko napadení systému útočníkem.

9. Zvýšení dostupnosti systému prostřednictvím redundance/replikace (HA). Zvýšení dostupnosti OU pro zpracovatele.

10. Zajištění pravidelného zálohování systému. Ochrana dostupnosti a integrity OU.

11. Zavedení disaster recovery plánu. DRP snižuje čas potřebný pro obnovu systému v případě havárie. Ochrana dostupnosti a integrity OU

12. Zavedení plánu zálohování. Ochrana dostupnosti a integrity OU.

13. Zavedení pravidelného testování obnovy ze zálohy. Ochrana dostupnosti a integrity OU.

14. Zavedení pravidelného vyhodnocování incidentů. Nezbytný předpoklad pro kontinuální zvyšování zabezpečení OU.

15. Zavedení pravidelného testování DR scénáře. Ochrana dostupnosti a integrity OU.

16. Zavedení pravidelného testování zranitelností. Nástroj pro měření úrovně bezpečnosti. Výsledkem je snížení úspěšnosti útoku.

Výše uvedené oblasti doporučení je možné rozdělit do 3 kategorií dle finanční a časové náročnosti zavedení:

- **Nízká náročnost zavedení**
  Jedná se o opatření, která lze velmi rychle aplikovat, obvykle s nízkými náklady na realizaci, přináší téměř okamžité výsledky. Platí pro oblasti 10–15.
- **Střední náročnost zavedení**
  Toto opatření vyžaduje analýzu proveditelnosti, předpokládáme však krátkodobou nebo střednědobou realizaci s částečným využitím externích dodavatelů. Platí pro oblasti 3–9, 16.
- **Vysoká náročnost zavedení**
  Toto opatření vyžaduje komplexní analýzu proveditelnosti prostřednictvím nového projektu, který má své nároky na časové (přesahující 6 měsíců) i finanční zdroje, které se mohou blížit k nákladům na generační obměnu technologie. Platí pro oblasti 1, 2.

2.4 Plán realizace

Při realizaci doporučení/ opatření jakožto závěrů analýzy dle tohoto dokumentu je vhodné postupovat dle priorit a návazností. V rámci přehledu nesouladu a doporučení je zpracován doporučený plán realizace. Pro každé doporučení v příloze č. 5 a 6 je uvedena prioritizace doporučení v rozmezí:

- 1 – doporučujeme realizovat doporučení okamžitě,
- 2 – doporučujeme začít realizovat v návaznosti na bod 1.

3 Posouzení

3.1 Souhrnná analýza připravenosti dle typů organizací

3.1.1 Kraje

Provedenou analýzou bylo zjištěno následující:

- V oblasti Procesů a opatření k ochraně dat – aktuální úroveň zralosti je u vybraných krajských úřadů na velmi odlišné úrovni. Osciluje mezi 32 % a 84 %. Analýzou se však podařilo identifikovat jak oblasti, ve kterých dosáhly všechny organizace velmi dobrých výsledků, tak i ty, ve kterých byly zjištěny zásadní nedostatky a úroveň zralosti je daleko za očekávanou úrovní. Nejlepších výsledků dosahují organizace v oblastech stanovení odpovědností, definice archivačních a skartačních pravidel a likvidace fyzických nosičů dat. Ochrana dat v procesech a přehled o zpracovávaných údajích je taktéž na velmi dobré úrovni.
- Naopak společné nedostatky byly identifikovány primárně v oblastech transparentnosti a informovanosti subjektů údajů, klasifikace dat, analýzy rizik a v oblasti zajištění naplnění práv subjektů údajů. Určité nedostatky byly zjištěny ve stavu řídicí dokumentace, samostatnou kapitolou je pak úroveň bezpečnostních požadavků ve zpracovatelských smlouvách.
- V oblasti Bezpečnostních opatření informací organizace přijaly řadu adekvátních opatření a aktuální úroveň zralosti je na mnohem lepší úrovni než u procesně organizačních opatření. Výsledky stavu připravenosti se pohybují v rozmezí 72 % - 100 %. Společným rysem je velmi dobrá připravenost v oblasti bezpečnosti sítí a síťových prvků, fyzické bezpečnosti a zálohování. Největší nedostatky byly naopak nalezeny v oblastech šifrování a logování.

3.1.1.1 Procesy a opatření k ochraně dat

3.1.1.1.1 Strategie a manuál k ochraně dat

Všechny organizace jsou schopny zodpovídat dotazy dozorového orgánu. Naopak v oblasti politik, strategie a cílů ochrany osobních údajů panují velké rozdíly. Některé organizace pak nepřijaly doposud žádná opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1 - 3,33

3.1.1.1.2 Směrnice pro zaměstnance

Všechny organizace mají zavedena pravidla pro tvorbu přístupových hesel a nakládání s nimi. I zde panují významné rozdíly ve stavu řídicí dokumentace, jedna organizace doposud nemá ani základní bezpečností pravidla. Nikde pak nebyly idenfitikována pravidla pro pohyb návštěv v objektech organizací.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,29 - 3

3.1.1.1.3 Odpovědnosti ve společnosti

Bezpečnostní role mají organizace definovány, stejně tak byly určeny jejich pravomoci a odpovědnosti. Ostatní povinné role však ve většině případů definovány nebyly (osoba odpovědná za ochranu OÚ, vlastníci dat, zpracovatelé).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,67 - 4,33

3.1.1.1.4 Činnosti zpracování

Z hlediska stavu připravenosti byly zjištěny zásadní rozdíly mezi jednotlivými organizacemi. Analýza prokázala u některých subjektů výskyt vysokých rizik a aktuální stav hluboko za očekávanou úrovní zralosti.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,75 - 3,50

3.1.1.1.5 Zpracovávané údaje

V této oblasti naopak dosahují organizace poměrně slušných výsledků. Všechny bez rozdílu určily časová rozmezí pro uchovávání dat a mají dokumentovaná pravidla pro jejich likvidaci (skartační a archivační řády). Stejně tak jsou známy a zadokumentovány právní tituly ke zpracování.

Očekávaná výstupní úroveň: 3

Aktuální výstupní úrovně: 2,25 - 5,00

3.1.1.1.6 Klasifikace dat

Tato oblast je všech organizacích pokryta minimálně, nebo vůbec, což sebou nese vysoká rizika. Pro dosažení shody s Nařízením je nutné klasifikovat jednotlivá data, ať již z hlediska důvěrnosti, dostupnosti a integrity, tak i z hlediska jejich specifikace. K jednotlivým klasifikačním stupňům musejí být pak zadokumentována pravidla pro bezpečnou manipulaci s nimi, pro jejich ochranu a úroveň zabezpečení.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,33 - 1,00

Oblast s výskytem vysokých rizik.

3.1.1.1.7 Infastruktura/přenos dat/tok dat

Organizace sice mají definována rozhraní mezi jednotlivými systémy, ale veškeré toky dat a jejich výměna mezi systémy doposud nebyly identifikovány a odpovídajícím způsobem zadokumentovány.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 - 1,33

Oblast zvýšených rizik v oblasti analýzy datových toků.

3.1.1.1.8 Transparentnost a informace o poskytnutí

Jedna z klíčových oblastí pro dosažení shody s Nařízením, kde však byly identifikovány zásadní nedostatky, a to ve všech organizacích. Zásady transparentnosti zpracování a povinnosti informování subjektů údajů doposud nebyly implementovány a je nutné okamžitě přistoupit k nápravě.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0 - 1

Oblast s výskytem vysokých rizik.

3.1.1.1.9 Analýza rizik

V oblasti řízení rizik jsou organizace rovněž hluboko za očekávanou úrovní zralosti. Je nutné definovat a nastavit proces řízení a zvládání rizik ve všech organizacích.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,50 - 2,33

Oblast zvýšených rizik v oblasti řízení rizik

3.1.1.1.10 Integrace procesu

Ochrana dat je v organizacích zvažována během všech procesů, naopak zvýšená pozornost by však měla být věnována ověřování souladu s příslušnou legislativou (compliance), v této oblasti organizace zaostávají.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,75 - 3,00

3.1.1.1.11 Procesy ochrany dat

Pro dosažení shody s Nařízením je nutné v této oblasti zahájit neprodleně kroky vedoucí k odstranění zásadních nedostatků. Organizace doposud nevytvořily jednotné náběrové místo pro příjem žádostí subjektů údajů. Nejsou definovány procesy k naplnění práv subjektů údajů (vzory žádostí, přístup, námitky, přenositelnost), chybí i relevantní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,07 - 2,33

Oblast zvýšených rizik

3.1.1.1.12 Porušení ochrany dat

V této oblasti byly zjištěny významné rozdíly ve stavu připravenosti jednotlivých organizací. Proces řízení incidentů nebyl v některých organizacích definován, pro dosažení shody s Nařízením je nutné tuto oblast adekvátně pokrýt a přijmout nezbytná opatření.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,50 - 3,50

3.1.1.1.13 Zpracovatelé

Většina organizací má definován proces řízení dodavatelů/zpracovatelů. V oblasti obsahu smluv s dodavateli však jsou všechny organizace v zásadní neshodě s Nařízením. Smlouvy totiž nezahrnují bezpečnostní požadavky ani opatření pro kontrolu plnění smluvních požadavků (sankce, audity, další kontrolní mechanismy).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 1,8

Oblast zvýšeného rizika v oblasti bezpečnostních požadavků ve smlouvách se zpracovateli.

3.1.1.1.14 Vědomí a trénink

V této oblasti rovněž panují významné rozdíly mezi úrovní zralosti. Byly identifkovány organizace, kde proces školení a vzdělávání zaměstnanců nebyl dosud implementován.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,40 - 3,60

3.1.1.1.15 Audit a neustálé zlepšování

Většina organizací nemá zavedeny kontrolní mechanismy a nemá implementován proces neustálého zlepšování. Těmto oblastem je nutné věnovat zvýšenou pozornost.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1 - 4,50

3.1.1.2 Opatření k ochraně informací

3.1.1.2.1 Obecné nároky na ochranná opatření

Organizace mají dokumentovaná bezpečnostní opatření k ochraně informací. Otázky anonymizace a pseudonymizace dat již byly ve většině případů nastoleny.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 3

3.1.1.2.2 Bezpečnost osobní a bezpečnost prostředí

Tato oblast je všech organizacích pokryta adekvátním způsobem, nebyly zjištěny neshody.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 3 - 5

3.1.1.2.3 Kontrola přístupu

I tato oblast je v organizacích na poměrně vysoké úrovni, přístup k OÚ a jejich zálohám je podmíněn silnými hesly.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,86 - 3,43

3.1.1.2.4 Bezpečnost sítě

Bezpečnost síťových prvků je v organizacích na vysoké úrovni. Přístupy z veřejné sítě jsou zabezpečeny pomocí firewallu. Byla implementována antivirová ochrana pro všechny klientské systémy. Většina organizací ale nevyužívá pokročilá opatření pro zabezpečení sítí.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,75 - 4,25

3.1.1.2.5 Dostupnost

V této oblasti nebyly identifikovány zásadní neshody. Všechny organizace přijaly opatření k zajištění těchto požadavků, většinou však bez adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 4

3.1.1.2.6 Bezpečnostní a nouzová opatření

V této oblasti nebyly identifikovány zásadní neshody. Všechny organizace přijaly opatření k zajištění těchto požadavků, většinou však bez adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 4

3.1.1.2.7 Integrita

V této oblasti nebyly identifikovány zásadní neshody. Všechny organizace přijaly opatření k zajištění těchto požadavků, většinou však bez adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 4

3.1.1.2.8 Odolnost

V této oblasti nebyly identifikovány zásadní neshody. Všechny organizace přijaly opatření k zajištění těchto požadavků, většinou však bez adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 4

3.1.1.2.9 Bezpečnost komunikace

Všechny organizace využívají řízení dálkového přístupu pomocí VPN. Naopak nikde nebyla vydána dokumentovaná pravidla pro bezpečný převoz dokumentů.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,25 - 2,75

3.1.1.2.10 Šifrování

Tato oblast je ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 2

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.1.2.11 Logování

Tato oblast je ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 2

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.2 Škola a školské zařízení

Provedenou analýzou bylo zjištěno následující:

- V oblasti Procesů a opatření k ochraně dat – aktuální úroveň zralosti je u vybraných organizací na velmi rozdílné úrovni. Osciluje mezi 15 % a 49 %. Některá opatření byla přijata, ale v mnoha oblastech existují významné neshody. Primárně se jedná o chybějící procesy řízení rizik a incidentů, nejsou definovány bezpečnostní požadavky na dodavatele, významné nedostatky byly zjištěny v oblasti transparentnosti a informování subjektů údajů o zpracování a v oblasti školení.
- V oblasti Bezpečnostních opatření informací organizace za očekávanou úrovní zralosti zaostávají výrazněji. Výsledky stavu připravenosti se pohybují v rozmezí 19 % až 43 %. Společným rysem je dobrá připravenost v oblasti bezpečnosti sítí, ale prakticky všechny ostatní oblasti nejsou adekvátně řešeny.

3.1.2.1 Procesy a opatření k ochraně dat

3.1.2.1.1 Strategie a manuál k ochraně dat

Klíčová oblast pro dosažení shody s Nařízením. Organizace definovaly politiky, strategie a cíle ochrany osobních údajů, chybí však adekvátní zadokumentování.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2

3.1.2.1.2 Směrnice pro zaměstnance

V této oblasti byly detekovány významné rozdíly, některé organizace přitom nedisponují ani základní sadou řídicí dokumentace. Obecně stavu dokumentace je nutné věnovat zvýšenou pozornost.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1 – 2,43

3.1.2.1.3 Odpovědnosti ve společnosti

V této oblasti byly zjištěny zásadní neshody s Nařízením, je nutné nezbytně přijmout adekvátní opatření a určit primárně osobu odpovědnou za ochranu OÚ a další bezpečnostní role.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,33 – 1,67

Oblast zvýšených rizik – definice odpovědné osoby a dalších bezpečnostních rolí.

3.1.2.1.4 Činnosti zpracování

Analýza prokázala u některých subjektů výskyt vysokých rizik a aktuální stav hluboko za očekávanou úrovní zralosti. Společným rysem je absence seznamu všech business procesů a chybějící účel zpracování.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0 – 1,75

Oblast výskytu vysokých rizik v oblasti identifikace procesů a dokumentovaného účelu zpracování.

3.1.2.1.5 Zpracovávané údaje

V této oblasti panují mezi jednotlivými organizacemi významné rozdíly. Společným rysem je však chybějící účel a právní titul všech zpracovatelských aktivit. Naopak v oblasti skartačních pravidel jsou organizace na adekvátní úrovni.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 – 2,50

Oblast zvýšeného rizika v oblasti účelu zpracování.

3.1.2.1.6 Klasifikace dat

Tato oblast je v organizacích pokryta minimálně. Pro dosažení shody s Nařízením je nutné klasifikovat jednotlivá data, ať již z hlediska důvěrnosti, dostupnosti a integrity, tak i z hlediska jejich

specifikace. K jednotlivým klasifikačním stupňům musejí být pak zadokumentována pravidla pro bezpečnou manipulaci s nimi, pro jejich ochranu a úroveň zabezpečení.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 2,00

Oblast zvýšených rizik.

3.1.2.1.7 Infastruktura/přenos dat/tok dat

V této oblasti doposud organizace nepřijaly žádná opatření, nedefinovaly rozhraní mezi jednotlivými systémy, veškeré toky dat a jejich výměnu mezi systémy.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast vysokých rizik v oblasti analýzy datových toků.

3.1.2.1.8 Transparentnost a informace o poskytnutí

Jedna z klíčových oblastí pro dosažení shody s Nařízením, kde však byly identifikovány zásadní nedostatky, a to ve všech organizacích. Subjekty údajů jsou sice informovány o zpracování OÚ a jejich právech, ale ostatní povinnosti o informování subjektů údajů doposud nebyly implementovány (automatizované zpracování, využití pro marketing, odebrání souhlasu atd.).

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,63 – 1,38

Oblast zvýšených rizik.

3.1.2.1.9 Analýza rizik

V oblasti řízení rizik jsou organizace rovněž hluboko za očekávanou úrovní zralosti. Je nutné definovat a nastavit proces řízení a zvládání rizik ve všech organizacích.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,17 – 0,67

Oblast vysokých rizik.

3.1.2.1.10 Integrace procesu

Tato oblast je na uspokojivé úrovni, ochrana dat je v organizacích zvažována během všech procesů, situačně se do procesů zapojuje odpovědná osoba. U některých organizací pak není zajištěno ověřování souladu s příslušnou legislativou (Compliance).

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,50 – 2,75

3.1.2.1.11 Procesy ochrany dat

V této oblasti panují mezi jednotlivými organizacemi významné rozdíly. Některé doposud nepřijaly žádná opatření vedoucí k zajištění práv subjektů údajů.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,40 – 2,67

Oblast vysokého rizika v oblasti naplnění práv subjektů údajů u některých organizací.

3.1.2.1.12 Porušení ochrany dat

Tato oblast je rovněž hluboko pod očekávanou úrovní zralosti. Proces řízení incidentů nebyl v organizacích definován, chybí pravidla pro sběr i vyhodnocování incidentů.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,25 – 1,50

Oblast zvýšeného rizika v oblasti řízení incidentů.

3.1.2.1.13 Zpracovatelé

Organizace nemají definován proces řízení dodavatelů/zpracovatelů – významná neshoda s Nařízením.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast vysokého rizika v oblasti řízení dodavatelů/zpracovatelů.

3.1.2.1.14 Vědomí a trénink

Žádná organizace nemá dokumentovaný výcvikový program. Školení samotné pak v určité podobě realizují všechny organizace, je ale nutné věnovat této oblasti zvýšenou pozornost.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,40 – 1,60

3.1.2.1.15 Audit a neustálé zlepšování

Organizace většinou nemají zavedeny kontrolní mechanismy a ani proces neustálého zlepšování. Nutno přijmout adekvátní opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast vysokého rizika u některých organizací.

3.1.2.2 Opatření k ochraně informací

3.1.2.2.1 Obecné nároky na ochranná opatření

Žádná organizace nemá dokumentovaná bezpečnostní opatření k ochraně informací. Otázky anonymizace a pseudonymizace dat jsou již zvažovány.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1 - 2

3.1.2.2.2 Bezpečnost osobní a bezpečnost prostředí

Zde byly zjištěny zásadní rozdíly mezi organizacemi, v některých organizacích byly identifikovány neshody a úroveň zralosti je hluboko pod očekávanou úrovní.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 2,33

Oblast zvýšeného rizika.

3.1.2.2.3 Kontrola přístupu

Tato oblast je v organizacích na uspokojivé úrovni, v oblasti řízení přístupů byla přijata řada opatření, i když určité nedostatky byly zjištěny v řídicí dokumentaci. Organizace rovněž nezajišťují přístup COÚ pomocí bezpečnostních opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,14 – 1,57

3.1.2.2.4 Bezpečnost sítě

Bezpečnost síťových prvků je v organizacích na dobré úrovni. Přístupy z veřejné sítě jsou zabezpečeny pomocí firewallu. Byla implementována antivirová ochrana pro všechny klientské systémy. Organizace ale nevyužívají pokročilá opatření pro zabezpečení sítí.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 3

3.1.2.2.5 Dostupnost

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,33

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.2.2.6 Bezpečnostní a nouzová opatření

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,33

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.2.2.7 Integrita

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,33

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.2.2.8 Odolnost

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,33

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.2.2.9 Bezpečnost komunikace

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,33

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.2.2.10 Šifrování

Tyto oblasti jsou ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,33 - 1

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.2.2.11 Logování

Tyto oblasti jsou ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,33 - 1

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.3 Zdravotnické zařízení

Provedenou analýzou bylo zjištěno následující:

- V oblasti Procesů a opatření k ochraně dat – aktuální úroveň zralosti je na přiměřené úrovni zralosti. Osciluje mezi 49 % a 51 %. Většina opatření již byla přijata, i když ne všechna mají odpovídající dokumentaci. V mnoha oblastech pak byly detekovány neshody, společné pro všechny organizace. Primárně se jedná o chybějící zadokumentování účelů zpracování pro všechny zpracovatelské aktivity, oblasti transparentnosti a informování subjektů údajů o zpracování, datové analýzy, analýzy rizik, řízení incidentů. Dalším společným rysem je absence bezpečnostních požadavků na dodavatele a nedostatečná úroveň školení.
- V oblasti Bezpečnostních opatření informací jsou organizace na různých úrovních stupně zralosti. Výsledky stavu připravenosti se pohybují v rozmezí 19 % až 56 %. Společným rysem je dobrá připravenost v oblasti bezpečnosti sítí, ale v ostatních oblastech je nutné zahájit neprodleně kroky k nápravě. Největší nedostatky byly zjištěny v oblastech šifrování a logování, principy bezpečnosti informací (důvěrnost, dostupnost, integrita) taktéž nejsou aplikovány dostatečně.

3.1.3.1 Procesy a opatření k ochraně dat

3.1.3.1.1 Strategie a manuál k ochraně dat

Klíčová oblast pro dosažení shody s Nařízením. Organizace definovaly politiky, strategie a cíle ochrany osobních údajů, v některých případech chybí adekvátní zadokumentování.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 3

3.1.3.1.2 Směrnice pro zaměstnance

Tato oblast je na slušné úrovni, organizace mají vydánu minimální sadu řídicí dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,43

3.1.3.1.3 Odpovědnosti ve společnosti

V této oblasti byly zjištěny neshody s Nařízením, je nutné nezbytně přijmout adekvátní opatření. Organizace sice určily osobu odpovědnou za ochranu OÚ, chybí však její větší zapojení do procesů ochrany dat a je nutné taktéž definovat další bezpečnostní role (fyzická bezpečnost, kryptografie, personální bezpečnost atd.).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,67

3.1.3.1.4 Činnosti zpracování

Analýza prokázala u některých subjektů výskyt rizik a aktuální stav pod očekávanou úrovní zralosti. Mezi nedostatky patří identifikace všech procesů a záznamy ohledně zpracovatelských činností.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,75 – 2,75

3.1.3.1.5 Zpracovávané údaje

V této oblasti dosáhly jednotlivé organizace dobrých výsledků. Identifikovaly původ OÚ, právní titul zpracování a archivační a skartační pravidla. Chybí však účel všech zpracovatelských aktivit.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,25 – 2,50

3.1.3.1.6 Klasifikace dat

Tato oblast je v organizacích pokryta adekvátním způsobem, určité nedostatky byly zjištěny ve stavu řídicí dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,00

Oblast zvýšených rizik.

3.1.3.1.7 Infastruktura/přenos dat/tok dat

V této oblasti organizace většinou nepřijaly žádná opatření, nedefinovaly rozhraní mezi jednotlivými systémy, veškeré toky dat a jejich výměnu mezi systémy.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 1

Oblast vysokých rizik v oblasti analýzy datových toků.

3.1.3.1.8 Transparentnost a informace o poskytnutí

Jedna z klíčových oblastí pro dosažení shody s Nařízením, kde však byly identifikovány nedostatky ve všech organizacích. Subjekty údajů jsou sice informovány o zpracování OÚ a jejich právech a organizace jsou schopny doložit legitimní záznamy souhlasů, ale ostatní povinnosti o informování

subjektů údajů doposud nebyly implementovány (automatizované zpracování, využití pro marketing, odebrání souhlasu atd.).

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1 – 1,38

Oblast zvýšených rizik pro oblast transparentnosti.

3.1.3.1.9 Analýza rizik

V oblasti řízení rizik jsou organizace rovněž hluboko pod očekávanou úrovní zralosti. Je nutné definovat a nastavit proces řízení a zvládání rizik ve všech organizacích.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,67 - 1

Oblast vysokých rizik.

3.1.3.1.10 Integrace procesu

Tato oblast je na uspokojivé úrovni, ochrana dat je v organizacích zvažována během všech procesů, situačně se do procesů zapojuje odpovědná osoba. U některých organizací pak není zajištěno ověřování souladu s příslušnou legislativou (Compliance).

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,50 – 2,75

3.1.3.1.11 Procesy ochrany dat

V této oblasti panují mezi jednotlivými organizacemi významné rozdíly. Některé doposud nepřijaly žádná opatření vedoucí k zajištění práv subjektů údajů, nemají vytvořeno jednotné náběrové místo, nedostatky panují také v oblasti vzorů a šablon a další podpůrné dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,20 – 2,67

Oblast vysokého rizika v oblasti naplnění práv subjektů údajů u některých organizací.

3.1.3.1.12 Porušení ochrany dat

Tato oblast je pod očekávanou úrovní zralosti. Organizace sice zavedly opatření pro identifikaci incidentů, ale samotný proces řízení incidentů nebyl v organizacích definován, chybí pravidla pro sběr i jejich vyhodnocování.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,25 – 1,50

Oblast zvýšeného rizika v oblasti řízení incidentů.

3.1.3.1.13 Zpracovatelé

I v této oblasti existují velké rozdíly ve stavu připravenosti, v některých nejsou dodavatelé/zpracovatelé řízeni. Společným rysem je absence bezpečnostních požadavků ve zpracovatelských smlouvách.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 2

Oblast zvýšeného rizika v oblasti řízení dodavatelů/zpracovatelů.

3.1.3.1.14 Vědomí a trénink

Žádná organizace nemá dokumentovaný výcvikový program. Školení samotné pak v určité podobě realizují všechny organizace, je ale nutné věnovat této oblasti zvýšenou pozornost.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1 – 1,60

Oblast zvýšeného rizika.

3.1.3.1.15 Audit a neustálé zlepšování

Organizace mají zavedeny kontrolní mechanismy i proces neustálého zlepšování. Chybí však adekvátní dokumentace a dokumentovaná pravidla.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,50 - 2

3.1.3.2 Opatření k ochraně informací

3.1.3.2.1 Obecné nároky na ochranná opatření

Žádná organizace nemá dokumentovaná bezpečnostní opatření k ochraně informací. Oblasti anonymizace a pseudonymizace dat jsou aktuálně pouze ve stadiu úvah.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 - 2

3.1.3.2.2 Bezpečnost osobní a bezpečnost prostředí

- Obecně je tato oblast pokryta nedostatečně, úroveň zralosti je hluboko pod očekávanou úrovní (omezení přístupu k OÚ a na zpracovatelská místa).
- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,33

Oblast zvýšeného rizika.

3.1.3.2.3 Kontrola přístupu

Tato oblast je v organizacích na uspokojivé úrovni, v oblasti řízení přístupů byla přijata řada opatření, i když určité nedostatky byly zjištěny v řídicí dokumentaci. Organizace rovněž nezajišťují přístup k COÚ pomocí bezpečnostních opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,14 – 2,29

3.1.3.2.4 Bezpečnost sítě

Bezpečnost síťových prvků je v organizacích na dobré úrovni. Přístupy z veřejné sítě jsou zabezpečeny pomocí firewallu. Byla implementována antivirová ochrana pro všechny klientské systémy. Některé organizace ale nevyužívají pokročilá opatření pro zabezpečení sítí.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2 - 3,50

3.1.3.2.5 Dostupnost, bezpečností a nouzová opatření, integrita, odolnost, bezpečnost komunikace

V těchto oblastech obecně organizace mírně zaostávají, primárně v oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity (dostupnost aktiv, zranitelnosti, hrozby a DR plány, logické a fyzické oddělení dat v systémech, monitoring výkonu a

reporting incidentů ohledně výkonu). Samostatnou kapitolou jsou pak neexistující pravidla bezpečné komunikace a manipulace s OÚ mimo organizace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 2

Oblast zvýšených rizik v oblasti bezpečnosti komunikace a bezpečnosti informací.

3.1.3.2.6 Šifrování a logování

Tyto oblasti jsou ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 1

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.4 Zařízení sociálních služeb

Provedenou analýzou bylo zjištěno následující:

- V oblasti Procesů a opatření k ochraně dat – aktuální úroveň zralosti je u vybraných organizací sociálních služeb obecně na velmi nízké úrovni zralosti. Osciluje mezi 9 % a 33 %. Prakticky ve všech oblastech byly zjištěny zásadní nedostatky.
- V oblasti Bezpečnostních opatření informací organizace za očekávanou úrovní zralosti zaostávají ještě výrazněji. Výsledky stavu připravenosti se pohybují v rozmezí 13 % až 19 %. Společným rysem je dobrá připravenost v oblasti bezpečnosti sítí, ale prakticky žádná z ostatních oblastí není adekvátně řešena.

3.1.4.1 Procesy a opatření k ochraně dat

3.1.4.1.1 Strategie a manuál k ochraně dat

Klíčová oblast pro dosažení shody s Nařízením. Je nutné definovat politiky, strategie a cíle ochrany osobních údajů. Některé organizace ale nepřijaly doposud žádná opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 1,67

3.1.4.1.2 Směrnice pro zaměstnance

Všechny organizace disponují alespoň základní sadou řídicí dokumentace. Byly však identifikovány významné nedostatky, především v oblasti bezpečnostních pravidel, nutno věnovat zvýšenou pozornost.

Očekávaná výstupní úroveň: 3

Aktuální výstupní úrovně: 1,29 – 1,71

3.1.4.1.3 Odpovědnosti ve společnosti

V této oblasti byly zjištěny zásadní neshody s Nařízením, je nutné nezbytně přijmout adekvátní opatření a určit odpovědné osoby pro jednotlivé oblasti.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,67

Oblast výskytu vysokých rizik – definice rolí a odpovědností.

3.1.4.1.4 Činnosti zpracování

Analýza prokázala u některých subjektů výskyt vysokých rizik a aktuální stav hluboko za očekávanou úrovní zralosti. Společným rysem je absence seznamu systémů, ve kterých dochází ke zpracování OÚ a chybějící účel zpracování.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0 – 1,50

Oblast výskytu vysokých rizik v oblasti dokumentovaného účelu zpracování.

3.1.4.1.5 Zpracovávané údaje

V této oblasti panují mezi jednotlivými organizacemi významné rozdíly. Společným rysem je však chybějící účel a právní titul všech zpracovatelských aktivit.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 2,75

Oblast zvýšeného rizika v oblasti účelu zpracování

3.1.4.1.6 Klasifikace dat

Tato oblast je všech organizacích pokryta minimálně, nebo vůbec, což sebou nese vysoká rizika. Pro dosažení shody s Nařízením je nutné klasifikovat jednotlivá data, ať již z hlediska důvěrnosti, dostupnosti a integrity, tak i z hlediska jejich specifikace. K jednotlivým klasifikačním stupňům

musejí být pak zadokumentována pravidla pro bezpečnou manipulaci s nimi, pro jejich ochranu a úroveň zabezpečení.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 1,00

Oblast s výskytem vysokých rizik.

3.1.4.1.7 Infastruktura/přenos dat/tok dat

- Další problémová oblast, existují organizace, které doposud nedefinovala rozhraní mezi jednotlivými systémy. Veškeré toky dat a jejich výměna mezi systémy doposud nebyly identifikovány a odpovídajícím způsobem zadokumentovány nikde.
- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 - 0,67

Oblast zvýšených rizik v oblasti analýzy datových toků.

3.1.4.1.8 Transparentnost a informace o poskytnutí

Jedna z klíčových oblastí pro dosažení shody s Nařízením, kde však byly identifikovány zásadní nedostatky, a to ve všech organizacích. Zásady transparentnosti zpracování a povinnosti informování subjektů údajů doposud nebyly implementovány a je nutné okamžitě přistoupit k nápravě.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0 – 1,25

Oblast s výskytem vysokých rizik.

3.1.4.1.9 Analýza rizik

V oblasti řízení rizik jsou organizace rovněž hluboko za očekávanou úrovní zralosti. Je nutné definovat a nastavit proces řízení a zvládání rizik ve všech organizacích.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0 – 0,83

Oblast vysokých rizik.

3.1.4.1.10 Integrace procesu

Tato oblast je velmi riziková, ochrana dat není v organizacích zvažována během všech procesů, ani při implementaci nových, není zajištěno zapojení odpovědných osob a nedochází k ověřování souladu s příslušnou legislativou (Compliance).

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0 – 0,75

Oblast vysokých rizik.

3.1.4.1.11 Procesy ochrany dat

Pro dosažení shody s Nařízením je nutné v této oblasti zahájit neprodleně kroky vedoucí k odstranění zásadních nedostatků. Organizace doposud nevytvořily jednotné náběrové místo pro příjem žádostí subjektů údajů. Nejsou definovány procesy k naplnění práv subjektů údajů (vzory žádostí, přístup, námitky, přenositelnost), chybí i relevantní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,27 – 0,47

Oblast vysokého rizika v oblasti naplnění práv subjektů údajů.

3.1.4.1.12 Porušení ochrany dat

Tato oblast je rovněž hluboko pod očekávanou úrovní zralosti. Proces řízení incidentů nebyl v organizacích definován, chybí pravidla pro identifikaci, sběr i vyhodnocování incidentů.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,25 – 0,75

Oblast vysokého rizika v oblasti řízení incidentů.

3.1.4.1.13 Zpracovatelé

Organizace nemají definován proces řízení dodavatelů/zpracovatelů – významná neshoda s Nařízením.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1

Oblast vysokého rizika v oblasti řízení dodavatelů/zpracovatelů.

3.1.4.1.14 Vědomí a trénink

Všechny organizace mají dokumentovaný výcvikový program. Trénink ale nezahrnuje specializovaná školení z ochrany OÚ a není vyhodnocován.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,40 – 1,60

3.1.4.1.15 Audit a neustálé zlepšování

Organizace nemají zavedeny kontrolní mechanismy a ani proces neustálého zlepšování. Nutno přijmout adekvátní opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast vysokého rizika.

3.1.4.2 Opatření k ochraně informací

3.1.4.2.1 Obecné nároky na ochranná opatření

Některé organizace mají dokumentovaná bezpečnostní opatření k ochraně informací. Otázky anonymizace a pseudonymizace dat doposud nebyly otevřeny.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 1,50

Oblast zvýšeného rizika pro oblast anonymizace a pseudonymizace.

3.1.4.2.2 Bezpečnost osobní a bezpečnost prostředí

Tato oblast není v organizacích pokryta adekvátním způsobem, byly zjištěny zásadní neshody.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,33

Oblast vysokého rizika.

3.1.4.2.3 Kontrola přístupu

I tato oblast je v organizacích na velmi nízké úrovni, přístup k OÚ a jejich zálohám není podmíněn silnými hesly, chybí politika i proces řízení přístupových oprávnění.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,43

Oblast vysokého rizika v oblasti řízení přístupů.

3.1.4.2.4 Bezpečnost sítě

Bezpečnost síťových prvků je v organizacích naopak na uspokojivé úrovni. Přístupy z veřejné sítě jsou zabezpečeny pomocí firewallu. Byla implementována antivirová ochrana pro všechny klientské systémy. Většina organizací ale nevyužívá pokročilá opatření pro zabezpečení sítí.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,75 – 2,25

3.1.4.2.5 Dostupnost

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,67

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.4.2.6 Bezpečnostní a nouzová opatření

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,67

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.4.2.7 Integrita

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,67

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.4.2.8 Odolnost

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,67

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.4.2.9 Bezpečnost komunikace

V této oblasti byly identifikovány významné neshody. V oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity jsou organizace výrazně za očekávaným stavem.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,67

Oblast vysokých rizik – chybí systém řízení bezpečnosti informací.

3.1.4.2.10 Šifrování

Tato oblast je ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,33

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.4.2.11 Logování

Tato oblast je ve všech organizacích hluboko za očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0 – 0,33

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.5 Kulturní zařízení

Provedenou analýzou bylo zjištěno následující:

- V oblasti Procesů a opatření k ochraně dat – aktuální úroveň zralosti je na dobré úrovni, pohybuje se v průměru okolo 50 %. Analýzou se podařilo identifikovat jak oblasti, ve kterých dosáhly organizace velmi dobrých výsledků, tak i ty, ve kterých byly zjištěny nedostatky a úroveň zralosti je daleko za očekávanou úrovní. Nejlepších výsledků dosahují organizace v oblastech činností zpracování, zpracování údajů a transparentnosti a informování subjektů údajů. Na dobré úrovni je též úroveň řídicí dokumentace. Naopak nedostatky byly identifikovány primárně v oblastech datových analýz, analýzy rizik, řízení auditů a školení.
- V oblasti Bezpečnostních opatření informací organizace přijaly řadu adekvátních opatření a z hlediska připravenosti jsou na dobré úrovni. Výsledky stavu připravenosti se pohybují okolo 73 %. Společným rysem je velmi dobrá připravenost v oblasti bezpečnosti sítí a síťových prvků, logování a řízení dostupnosti. Největší nedostatky byly naopak nalezeny v oblasti šifrování.

3.1.5.1 Procesy a opatření k ochraně dat

3.1.5.1.1 Strategie a manuál k ochraně dat

Organizace jsou na velmi dobré úrovni, politika ochrany osobních údajů, strategie a cíle vedoucí k ochraně dat byly vydány. Zodpovězení dotazů dozorového orgánu je možné splnit.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 3,67

3.1.5.1.2 Směrnice pro zaměstnance

Organizace mají k dispozici dokumentovaná uživatelská pravidla pro oblast ochrany osobních údajů a také základní sadu bezpečnostní dokumentace. Nástroj smluvního závazku utajení v podobě NDA organizace využívají.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,43

3.1.5.1.3 Odpovědnosti ve společnosti

Organizace určily osoby odpovědné za ochranu osobních údajů a stanovily jejich odpovědnosti. Ostatní role odpovědné za ochranu osobních údajů v systémech (vlastník, zpracovatel apod.) také byly definovány. Chybí pouze bezpečnostní role.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,67

3.1.5.1.4 Činnosti zpracování

Organizace určily business procesy, včetně procesů, ve kterých dochází ke zpracování osobních dat. Přehledy systémů, ve kterých dochází ke zpracování osobních údajů, jsou známy. Záznamy o činnostech zpracování nemají organizace v dokumentované podobě.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 2,50

3.1.5.1.5 Zpracovávané údaje

V této oblasti dosahují organizace dobrých výsledků. Všechny určily časová rozmezí pro uchovávání dat a mají dokumentovaná pravidla pro jejich likvidaci (skartační a archivační řády). Stejně tak jsou známy a zadokumentovány právní tituly ke zpracování.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,75

3.1.5.1.6 Klasifikace dat

Tato oblast je v organizacích nedostatečně pokryta. Pro dosažení shody s Nařízením je nutné klasifikovat jednotlivá data, ať již z hlediska důvěrnosti, dostupnosti a integrity, tak i z hlediska jejich specifikace. K jednotlivým klasifikačním stupňům musejí být pak zadokumentována pravidla pro bezpečnou manipulaci s nimi, pro jejich ochranu a úroveň zabezpečení.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,67

3.1.5.1.7 Infastruktura/přenos dat/tok dat

Organizace sice mají definována rozhraní mezi jednotlivými systémy, ale veškeré toky dat a jejich výměnu mezi systémy doposud neidenfitikovaly.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67

Oblast vysokých rizik v oblasti analýzy datových toků.

3.1.5.1.8 Transparentnost a informace o poskytnutí

Organizace definovaly procesy poskytování informací subjektům údajů o zpracování jejich osobních údajů. Vedou i evidenci souhlasů se zpracováním, do souhlasů již byly adaptovány požadavky Nařízení. Ostatní povinnosti vyplývající z Nařízení (čl. 13 a 14) nebyly doposud implementovány.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 2,50

3.1.5.1.9 Analýza rizik

V oblasti řízení rizik jsou organizace hluboko pod očekávanou úrovní zralosti. Je nutné definovat a nastavit proces řízení a zvládání rizik ve všech organizacích.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,50

Oblast vysokých rizik v oblasti řízení rizik.

3.1.5.1.10 Integrace procesu

Organizace požadavky na ochranu dat adekvátně zvažují ve všech procesech, i při implementaci nových procesů. Při zavádění nových zpracovatelských činností je situačně prováděno ověřování souladu s příslušnou legislativou. Odpovědné osoby se příležitostně zapojuje do procesu ochrany osobních údajů.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 2,25

3.1.5.1.11 Procesy ochrany dat

Organizace vytvořily jednotné náběrové místo pro příjem žádostí subjektů údajů. Nejsou ale zavedeny dokumentované postupy a nástroje pro řízení přístupů a pro skartaci dat, pro naplnění práv subjektů údajů (výmaz, přístup, přenositelnost, námitku, procedury pro zacházení s žádostmi, technická opatření pro dodržení skartačních lhůt, procesy kontroly přenosů dat apod.).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,60

3.1.5.1.12 Porušení ochrany dat

Organizace nemají vytvořeny dokumentované postupy pro detekci porušení ochrany dat (identifikace, sběr a vyhodnocování incidentů). Bez těchto procesů nelze dosáhnout shody s Nařízením.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,25

Oblast vysokého rizika v oblasti řízení incidentů.

3.1.5.1.13 Zpracovatelé

Organizace mají pravidla pro výběr a hodnocení dodavatelů (zpracovatelů). Písemné kontrakty ale nezahrnují opatření pro kontrolu plnění smluvních požadavků (sankce, audity, další kontrolní mechanismy). Chybí i písemný seznam zpracovatelů.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2

Oblast zvýšeného rizika v oblasti bezpečnostních požadavků ve smlouvách se zpracovateli.

3.1.5.1.14 Vědomí a trénink

Organizace nedefinovaly a neschválily výcvikový program. Školení z ochrany osobních údajů nejsou realizována a vyhodnocována.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,60

Oblast vysokého rizika.

3.1.5.1.15 Audit a neustálé zlepšování

Organizace nemají zavedeny kontrolní mechanismy a principy neustálého zlepšování. Efektivita opatření přijatých k ochraně osobních údajů není vyhodnocována a reportována vedení společnosti, chybí i adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50

Oblast vysokého rizika.

3.1.5.2 Opatření k ochraně informací

3.1.5.2.1 Obecné nároky na ochranná opatření

Organizace mají zavedeny dokumentovaná bezpečnostní opatření k ochraně informací. V oblasti anonymizace a pseudonymizace dat již mají dokumentovaná pravidla.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 3

3.1.5.2.2 Bezpečnost osobní a bezpečnost prostředí

Z hlediska fyzické bezpečnosti prostředí jsou organizace za dobré úrovni. Zavedly kontrolní mechanismy řízení přístupů, byla definována pravidla pro pohyb v režimových oblastech a zpracovatelských místech a jsou prováděny pravidelné kontroly

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2

3.1.5.2.3 Kontrola přístupu

Tato oblast je v organizacích na poměrně vysoké úrovni, požadavky na bezpečné řízení přístupových oprávnění k jednotlivým systémům a osobním datům jsou naplněny, zjištěny byly jen drobné nedostatky v dokumentaci.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,43

3.1.5.2.4 Bezpečnost sítě

Bezpečnost síťových prvků je v organizacích na vysoké úrovni. Přístupy z veřejné sítě jsou zabezpečeny pomocí firewallu. Byla implementována antivirová ochrana pro všechny klientské systémy. Většina organizací ale nevyužívá pokročilá opatření pro zabezpečení sítí.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 3,25

3.1.5.2.5 Dostupnost

V této oblasti obecně organizace mírně zaostávají. V oblasti dostupnosti jsou ovšem na dobré úrovni zralosti. Určité nedostatky byly zjištěny v oblastech, zálohování, zjišťování zranitelností a hrozeb, SLA se zpracovateli atd.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 2,75

3.1.5.2.6 Bezpečnostní a nouzová opatření

V této oblasti obecně organizace mírně zaostávají. V oblasti dostupnosti jsou ovšem na dobré úrovni zralosti. Určité nedostatky byly zjištěny v oblastech, zálohování, zjišťování zranitelností a hrozeb, SLA se zpracovateli atd.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 2,75

3.1.5.2.7 Integrita

V této oblasti obecně organizace mírně zaostávají. V oblasti dostupnosti jsou ovšem na dobré úrovni zralosti. Určité nedostatky byly zjištěny v oblastech, zálohování, zjišťování zranitelností a hrozeb, SLA se zpracovateli atd.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 2,75

3.1.5.2.8 Odolnost

V této oblasti obecně organizace mírně zaostávají. V oblasti dostupnosti jsou ovšem na dobré úrovni zralosti. Určité nedostatky byly zjištěny v oblastech, zálohování, zjišťování zranitelností a hrozeb, SLA se zpracovateli atd.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 2,75

3.1.5.2.9 Bezpečnost komunikace

V této oblasti obecně organizace mírně zaostávají. V oblasti dostupnosti jsou ovšem na dobré úrovni zralosti. Určité nedostatky byly zjištěny v oblastech, zálohování, zjišťování zranitelností a hrozeb, SLA se zpracovateli atd.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67 – 2,75

3.1.5.2.10 Šifrování

Tyto oblasti jsou ve všech organizacích hluboko pod očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.5.2.11 Logování

Tato oblast je v organizacích nad očekávanou úrovní zralosti.

- Očekávaná výstupní úroveň: 3

Aktuální výstupní úrovně: 3,3

3.1.6 Oblast dopravní obslužnosti

Provedenou analýzou bylo zjištěno následující:

- V oblasti Procesů a opatření k ochraně dat – aktuální úroveň zralosti je na uspokojivé úrovni, pohybuje se v průměru okolo 35 %. Analýzou se podařilo identifikovat jak oblasti, ve kterých dosáhly organizace velmi dobrých výsledků, tak i ty, ve kterých byly zjištěny nedostatky a úroveň zralosti je daleko za očekávanou úrovní. Nejlepších výsledků dosahují organizace v oblastech zpracování údajů.
- Naopak nedostatky byly identifikovány primárně v oblastech transparentnosti a informovanosti subjektů údajů, stanovení odpovědností, analýzy rizik a školení.
- V oblasti Bezpečnostních opatření informací organizace přijaly řadu adekvátních opatření. Výsledky stavu připravenosti se pohybují okolo 40 %. Společným rysem je velmi dobrá připravenost v oblasti bezpečnosti sítí a síťových prvků. Největší nedostatky byly naopak nalezeny v oblastech šifrování a logování.

3.1.6.1 Procesy a opatření k ochraně dat

3.1.6.1.1 Strategie a manuál k ochraně dat

Klíčový dokument – politika ochrany osobních údajů – byl sice definován, ale doposud neexistuje v písemné podobě. Organizace si rovněž nestanovily strategie a cíle vedoucí k ochraně dat. Zajištění zodpovězení dotazů dozorového orgánu je možné splnit, ale chybí adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,67

3.1.6.1.2 Směrnice pro zaměstnance

Organizace zatím nevydaly dokumentovaná uživatelská pravidla pro oblast ochrany osobních údajů. V oblasti bezpečnostní dokumentace chybí směrnice, nástroj smluvního závazku utajení v podobě NDA organizace nevyužívají.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,29

3.1.6.1.3 Odpovědnosti ve společnosti

Bezpečnostní role nemají organizace definovány, nejsou určeny jejich pravomoci a odpovědnosti. Ostatní povinné role také definovány nebyly (osoba odpovědná za ochranu OÚ, vlastníci dat, zpracovatelé).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Jedná se o oblast vysokých rizik.

3.1.6.1.4 Činnosti zpracování

Organizace znají business procesy, avšak bez procesů, ve kterých dochází ke zpracování osobních dat. Neexistuje dokumentovaný seznam IT systémů. Záznamy o činnostech zpracování organizace nemají.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,25

3.1.6.1.5 Zpracovávané údaje

V této oblasti naopak dosahují organizace dobrých výsledků. Všechny bez rozdílu určily časová rozmezí pro uchovávání dat a mají dokumentovaná pravidla pro jejich likvidaci (skartační a archivační řády). Stejně tak jsou známy a zadokumentovány právní tituly ke zpracování.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 3

3.1.6.1.6 Klasifikace dat

Tato oblast je všech organizacích pokryta minimálně, nebo vůbec, což sebou nese vysoká rizika. Pro dosažení shody s Nařízením je nutné klasifikovat jednotlivá data, ať již z hlediska důvěrnosti, dostupnosti a integrity, tak i z hlediska jejich specifikace. K jednotlivým klasifikačním stupňům musejí být pak zadokumentována pravidla pro bezpečnou manipulaci s nimi, pro jejich ochranu a úroveň zabezpečení.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,33

Oblast s výskytem vysokých rizik.

3.1.6.1.7 Infastruktura/přenos dat/tok dat

Organizace nemají definována ani rozhraní mezi jednotlivými systémy, ani veškeré toky dat a jejich výměnu mezi systémy.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast vysokých rizik v oblasti analýzy datových toků.

3.1.6.1.8 Transparentnost a informace o poskytnutí

Jedna z klíčových oblastí pro dosažení shody s Nařízením, kde však byly identifikovány nedostatky. Zásady transparentnosti zpracování a povinnosti informování subjektů údajů doposud nebyly implementovány a je nutné okamžitě přistoupit k nápravě.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0

Oblast s výskytem vysokých rizik.

3.1.6.1.9 Analýza rizik

V oblasti řízení rizik jsou organizace rovněž hluboko za očekávanou úrovní zralosti. Je nutné definovat a nastavit proces řízení a zvládání rizik ve všech organizacích.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,33

Oblast vysokých rizik v oblasti řízení rizik

3.1.6.1.10 Integrace procesu

Organizace požadavky na ochranu dat adekvátně zvažují při implementaci nových procesů. Při zavádění nových zpracovatelských činností je situačně prováděno ověřování souladu s příslušnou legislativou. Odpovědné osoby se příležitostně zapojuje do procesu ochrany osobních údajů.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 1,75

3.1.6.1.11 Procesy ochrany dat

Organizace vytvořily jednotné náběrové místo pro příjem žádostí subjektů údajů. Nejsou ale zavedeny dokumentované postupy a nástroje pro řízení přístupů a pro skartaci dat, pro naplnění práv subjektů údajů (pro výmaz, přístup, přenositelnost, námitku apod.).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,27

3.1.6.1.12 Porušení ochrany dat

Organizace nemají vytvořeny dokumentované postupy pro detekci porušení ochrany dat (identifikace, sběr a vyhodnocování incidentů). Bez těchto procesů nelze dosáhnout shody s Nařízením.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0,75

3.1.6.1.13 Zpracovatelé

Organizace mají pravidla pro výběr a hodnocení dodavatelů (zpracovatelů). Písemné kontrakty ale nezahrnují opatření pro kontrolu plnění smluvních požadavků (sankce, audity, další kontrolní mechanismy). Chybí i písemný seznam zpracovatelů.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,4

Oblast zvýšeného rizika v oblasti bezpečnostních požadavků ve smlouvách se zpracovateli.

3.1.6.1.14 Vědomí a trénink

Byly identifkovány organizace, kde proces školení a vzdělávání zaměstnanců nebyl dosud implementován, nutné přijmout adekvátní opatření.

- Očekávaná výstupní úroveň: 4
- Aktuální výstupní úrovně: 0

Oblast vysokého rizika.

3.1.6.1.15 Audit a neustálé zlepšování

Organizace nemají zavedeny kontrolní mechanismy a implementován proces neustálého zlepšování. Neshoda s Nařízením.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast vysokého rizika.

3.1.6.2 Opatření k ochraně informací

3.1.6.2.1 Obecné nároky na ochranná opatření

Organizace mají stanovena bezpečnostní opatření k ochraně informací. Otázky anonymizace a pseudonymizace dat již byly nastoleny, chybí adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2

3.1.6.2.2 Bezpečnost osobní a bezpečnost prostředí

Z hlediska fyzické bezpečnosti prostředí jsou organizace za očekáváním. Nejsou využívány kontrolní mechanismy řízení přístupů, nebyla vytvořena pravidla pro pohyb v režimových oblastech a zpracovatelských místech a nejsou prováděny pravidelné kontroly.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,67

3.1.6.2.3 Kontrola přístupu

Tato oblast je v organizacích na poměrně vysoké úrovni, požadavky na bezpečné řízení přístupových oprávnění k jednotlivým systémům a osobním datům jsou naplněny, chybí jen adekvátní dokumentace.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 1,57

3.1.6.2.4 Bezpečnost sítě

Bezpečnost síťových prvků je v organizacích na vysoké úrovni. Přístupy z veřejné sítě jsou zabezpečeny pomocí firewallu. Byla implementována antivirová ochrana pro všechny klientské systémy. Většina organizací ale nevyužívá pokročilá opatření pro zabezpečení sítí.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 2,75

3.1.6.2.5 Dostupnost

V této oblasti organizace obecně mírně zaostávají, primárně v oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity (dostupnost aktiv, SLA se zpracovateli, zálohování, monitoring výkonu).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 – 1,75

3.1.6.2.6 Bezpečnostní a nouzová opatření

V této oblasti organizace obecně mírně zaostávají, primárně v oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity (dostupnost aktiv, SLA se zpracovateli, zálohování, monitoring výkonu).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 – 1,75

3.1.6.2.7 Integrita

V této oblasti organizace obecně mírně zaostávají, primárně v oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity (dostupnost aktiv, SLA se zpracovateli, zálohování, monitoring výkonu).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 – 1,75

3.1.6.2.8 Odolnost

V této oblasti organizace obecně mírně zaostávají, primárně v oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity (dostupnost aktiv, SLA se zpracovateli, zálohování, monitoring výkonu).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 – 1,75

3.1.6.2.9 Bezpečnost komunikace

V této oblasti organizace obecně mírně zaostávají, primárně v oblastech klíčových pro zajištění bezpečnosti informací a dodržení zásad důvěrnosti, dostupnosti a integrity (dostupnost aktiv, SLA se zpracovateli, zálohování, monitoring výkonu).

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0,50 – 1,75

3.1.6.2.10 Šifrování

Tato oblast je ve všech organizacích hluboko pod očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.1.6.2.11 Logování

Tato oblast je ve všech organizacích hluboko pod očekávanou úrovní zralosti. Organizace nezahájily implementaci potřebných opatření.

- Očekávaná výstupní úroveň: 3
- Aktuální výstupní úrovně: 0

Oblast výskytu vysokého rizika v oblasti ochrany proti kompromitaci dat.

3.2 Přehled zpracovávaných OÚ

Mapování zpracování konkrétních osobních údajů v rámci činností jednotlivých agend krajů a právnických osob zřizovanými kraji vychází z dotazníkových šetření.

V rámci přehledu jsou uvedeny činnosti, při nichž dochází ke zpracování osobních údajů, kategorie a rozsah zpracovávaných osobních údajů, kategorie subjektů údajů, účel zpracování osobních údajů, kategorie příjemců a doba uložení. Tento dokument nepředstavuje úplný výčet vykonávaných činností, při kterých dochází ke zpracování osobních údajů ani úplný rozsah zpracovávaných osobních údajů (viz přílohy č. 1 a 2).

Z provedeného dotazníkového šetření vyplývá, že osoby podílející se na zpracování osobních údajů nemají dostatečné povědomí o rozsahu činností, při nichž dochází ke zpracování osobních údajů. Z dotazníků a následné konzultace dotazníků s kontaktními osobami dále vyplynulo, že osoby podílející se na zpracování osobních údajů nejsou dostatečně obeznámené s problematikou ochrany osobních údajů a z toho důvodu nejsou v mnoha případech schopny uvést jednotlivé položky mapování zpracování osobních údajů v rámci jejich organizace. Na základě porovnání těchto závěrů mezi kraji a právnickými osobami zřizovanými kraji lze konstatovat, že míra povědomí o povinnostech ochrany osobních údajů je v případě právnických osob zřizovaných krajem významně nižší. S ohledem na tato zjištění doporučujeme provést školení zaměstnanců a dalších osob, které se podílí na zpracování osobních údajů.

3.3 Zpracování OÚ/COÚ v informačních systémech

Mapování zpracování konkrétních OÚ/COÚ v rámci činností jednotlivých agend, s využitím konkrétních informačních systémů, je uvedeno pro kraje v kapitole 3.3.1 a pro právnické osoby

zřizované kraji v kapitole 3.3.2. Přehled vychází z odpovědí jednotlivých respondentů v organizačním a právním dotazníku a přehledu IT systémů.

3.3.1 Kraje

Mapování zpracování konkrétních OÚ/COÚ v rámci činností jednotlivých agend krajů je uvedeno v následujícím přehledu.

Agenda	Typ IS	Přehled OÚ
Doprava		
	Ekonomický systém	jméno, příjmení, titul, adresa, datum narození, rodné číslo, kontaktní údaje, IČ
	Ostatní	jméno, příjmení, titul, adresa, datum narození, rodné číslo, kontaktní údaje, IČ
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, titul, datum narození, rodné číslo, datum narození, adresa trvalého bydliště jiné údaje: kontakt (tel., e-mail), IČO popisné údaje: registrační značky vozidel
	Agendové IS, Evidence	adresní a identifikační údaje: jméno, příjmení, titul, datum narození, rodné číslo, datum narození, adresa trvalého bydliště jiné údaje: kontakt (tel., e-mail), IČO popisné údaje: registrační značky vozidel
	Sítové disky	jméno, příjmení, datum narození, místo trvalého pobytu, případně doručovací adresa
Školství, mládež, tělovýchova		
	Agendové IS, Evidence	jméno, příjmení, titul, bydliště, datum narození, rodné číslo, číslo OP, číslo cestovního pasu, případně další údaje uvedené žadatelem, plat, průměrný měsíční výdělek, výše odměn, výše osobního příplatku, doba započitatelné praxe; zaměstnavatel, e-mail, telefon, trestní bezúhonnost, sídlo, IČ, DIČ, bankovní spojení, další údaje nezbytné pro jednání o uzavření či změně smlouvy a pro plnění smlouvy, funkce, údaje z veřejně přístupných evidencí, anotace ocenění, zákonný zástupce nezletilého dítěte a žáka, uzavřené vzdělání, zájem o pracovní místo, místo podnikání
	Ekonomický systém	jméno, příjmení, datum narození, adresa, název a sídlo vysílající školy, název a sídlo přijímající školy, údaje o průběhu a výsledcích závěrečné nebo maturitní zkoušky nebo absolutoria, státní příslušnost, rodné číslo, výše příjmů, umístění žáka v soutěži, adresa zaměstnavatele, e-mail, telefonický kontakt, návrh platu
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, titul, datum narození, místo trvalého pobytu, adresa pro doručování účastníka řízení, jméno, příjmení, titul, místo trvalého pobytu, adresa pro doručování zástupce účastníka řízení nebo zmocněnce, bankovní a telefonní spojení, e-mail jiné údaje: údaje o dosaženém vzdělání a údaje o výsledcích vzdělávání žadatele
Životní prostředí a zemědělství	**Agendové IS, Evidence**	
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, datum narození, adresa trvalého bydliště, kontaktní adresa, rodné číslo, číslo OP citlivé údaje: odsouzení pro trestný čin popisné údaje: odborné znalosti
	Ekonomický systém	datum narození, rodné číslo, adresa, podpisy

Agenda	Typ IS	Přehled OÚ
	Agendové IS, Evidence	jméno, datum narození, trvalý pobyt, IČ, jméno, identifikační číslo, lokační údaje, adresa, zdravotní stav
Územní plánování + stavební úřad	**Agendové IS, Evidence**	
	Agendové IS, Evidence	jméno, příjmení, titul, adresa, adresa pro doručování, e-mailová adresa, telefonní číslo, návrh odměn, sídlo, datum narození, IČ, DIČ, bankovní spojení; funkce, kontaktní údaje, údaje z veřejně přístupných evidencí.
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, datum narození, adresa místa trvalého pobytu nebo adresa bydliště a adresa pro doručování, IČ
Kultura a památková péče	**Agendové IS, Evidence**	
	Agendové IS, Evidence	jméno, příjmení, titul, bydliště, datum narození, rodné číslo, výše platu, doba započitatelné praxe, bankovní spojení
	Spisová služba	jméno, příjmení, titul, datum narození, rodné číslo, místo trvalého pobytu, bankovní spojení
	Ekonomický systém	jméno, datum a místo narození, adresa trvalého bydliště, č. OP
Odbor regionálního rozvoje (cestovní ruch)	**Agendové IS, Evidence**	
	Agendové IS, Evidence	titul, jméno, příjmení, bydliště, sídlo, datum a místo narození, IČ, DIČ, rodné číslo, bankovní spojení, další údaje nezbytné pro jednání o uzavření či změně smlouvy a pro plnění smlouvy, funkce, kontaktní údaje, údaje z veřejně přístupných evidencí, údaje o nemovitosti, výše platu, funkční náplň, mzdové údaje, číslo OP, číslo cestovního pasu
	Sítové disky	adresní a identifikační údaje: jméno, příjmení, adresa trvalého bydliště, datum narození, rodné číslo jiné údaje: kontakt (tel., e-mail), bankovní spojení, údaje o předchozí registraci na úřadu práce, údaje o splnění rekvalifikačního kurzu
Odbor kontroly (přezkum hospodaření obcí atd.)	**Agendové IS, Evidence**	
	Ekonomický systém	jméno, příjmení, bydliště, datum narození, vlastnické právo k nemovitosti
	Agendové IS, Evidence	jméno, příjmení, bydliště, datum narození, vlastnické právo k nemovitosti
Investice a majetek	**Agendové IS, Evidence**	
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, datum narození, adresa místa trvalého pobytu, sídlo, jiné údaje: IČ, DIČ, Informace o zápisu v ŽL nebo OR či jiném rejstříku, bankovní spojení, telefon, fax, e-mail, datová schránka
	Sítové disky	adresní a identifikační údaje: jméno, příjmení, datum narození, adresa místa trvalého pobytu, sídlo, jiné údaje: IČ, DIČ, Informace o zápisu v ŽL nebo OR či jiném rejstříku, bankovní spojení, telefon, fax, e-mail, datová schránka
Odbor kanceláře hejtmanky a vnějších vztahů	**Agendové IS, Evidence**	
	Kancelářský SW	datum narození, pohlaví, č. osobního dokladu, sídlo firmy, bydliště, zaměstnání.
	Ekonomický systém	datum narození, pohlaví, č. osobního dokladu, sídlo firmy, bydliště, zaměstnání.

Agenda	Typ IS	Přehled OÚ
	Spisová služba	jméno, příjmení, titul, datum narození, adresa trvalého pobytu ev. adresa pro doručování, rodné číslo, kontakty (tel., e-mail), členství v politické straně/hnutí, zaměstnání, bankovní spojení
	Agendové IS, Evidence	jméno, příjmení, titul, datum narození, adresa trvalého pobytu ev. adresa pro doručování, rodné číslo, kontakty (tel., e-mail), členství v politické straně/hnutí, zaměstnání
Odbor podpory řízení KÚ (spisová služba)	**Agendové IS, Evidence**	
	Ekonomický systém	jméno a příjmení, datum narození, státní občanství, pohlaví, adresa, zraněná část těla, popis vzniku zranění, název společnosti, bydliště,
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, rok narození, obec, zdravotní stav, trestní bezúhonnost jiné údaje: výše a účel poskytnutých veřejných prostředků
Odbor kanceláře ředitele úřadu	**Agendové IS, Evidence**	
	Nespecifikované	adresní a identifikační údaje: jméno, příjmení, titul, rodné příjmení, datum a místo narození, rodinný stav, rodné číslo, státní příslušnost, adresa trvalého bydliště, číslo OP, počet dětí, předchozí zaměstnání, zdravotní pojišťovna, osoby se zdravotním postižením, odměna za výkon funkce, bankovní spojení, čestné prohlášení o členství v řídícím, dozorčím nebo kontrolním orgánu právnické osoby, jejímž předmětem činnosti je podnikání a prohlášení o vykonávání jiné výdělečné činnosti, identifikační údaje rodinných příslušníků a ostatních vyživovaných osob
Odbor legislativní a právní	**Agendové IS, Evidence**	
	Agendové IS, Evidence	jméno, příjmení, datum a místo narození, trvalý pobyt, adresa pro doručování, e-mail, telefon, občanský průkaz, titul, rodné číslo, bydliště, údaj o trestní bezúhonnosti, údaje z čestného prohlášení, IČ, DIČ, číslo účtu, název peněžitého ústavu, údaje z veřejně přístupných evidencí, zdravotní pojišťovna, číslo účtu, zdroj příjmů - informace o platových poměrech, sídlo, údaje o majetku, politická příslušnost, rodinný stav, počet dětí, vzdělání, povolání, fotografie, projev, informace o občanství kraje
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, rodné příjmení, datum a místo narození, včetně státu, státní příslušnost, adresa trvalého bydliště, adresa posledního trvalého bydliště na území ČR, rodné číslo, pohlaví, datum a způsob nabytí / pozbytí st. občanství ČR
	Ekonomický systém	jméno, adresa, titul, trvalé bydliště, doručovací adresa, datum narození, rodné číslo, e-mail, IČ, číslo účtu, plátce mzdy; telefonní číslo – soukromé i pracovní, DIČ, číslo účtu, příjem ze zaměstnání a majetkové poměry v rámci podaného čestného prohlášení dle zákona o střetu zájmů

Agenda	Typ IS	Přehled OÚ
Krajský živnostenský úřad (+ veřejné sbírky, občanské agendy, přestupky)	**Agendové IS, Evidence**	
	Ekonomický systém	jméno, rodné příjmení, příjmení, datum a místo narození, adresa trvalého pobytu, funkce, vlastnoruční podpis, rodné číslo, státní příslušnost, pobyt na/mimo území ČR, vzdělání, email, telefonní číslo, věk, povolání, politická angažovanost, místo podnikání, místa provozoven, IČ/DIČ, bezúhonnost, zdravotní stav, pohlaví, datum vzniku/zániku manželství/regi. partnerství, datum úmrtí, způsobilost k právním úkonům, svéprávnost, rodinný stav, osvojení, určení či popření otcovství, služba v armádě a jiných ozbrojených složkách, sexuální život, rasový či etnický původ, členství v odborových organizacích, náboženství a filozofické přesvědčení, majetkové poměry,
	Spisová služba	Jméno, příjemní, trvalý pobyt doručovací adresa, státní občanství, jméno, příjmení, trvalý pobyt (veřejné sbírky, správní řízení, pohřebnictví, dobrovolné svazky obcí)
	Agendové IS, Evidence	jméno, příjmení, datum narození, rodné číslo, adresa trvalého pobytu, adresa pro doručování, státní občanství, stav
Odbor sociálních věcí	**Agendové IS, Evidence**	
	Nespecifikované	jméno a příjmení, datum a místo narození, trvalý pobyt, příp. bydliště, příp. adresa pro doručování, příp. další údaje uvedené žadatelem, st. příslušnost, majetkové poměry, sídlo a IČ (podnikající FO), prac. zařazení, kontakt /e-mail, telefon/, rodné číslo, občanství, číslo OP, příp. jiného dokladu, sociální poměry, profese, adresa zaměstnavatele, charakteristika osobnosti, motivace a předpoklad vychovávat dítě, stabilita manželského vztahu, údaj o závazcích, vlastnické nebo jiné právo k nemovitostem; soc. pracovník poskytovatele - jméno a příjmení, trvalý pobyt, údaj o vzdělání, odsouzení za přestupek
	Ekonomický systém	údaje podle § 10a odst. 3 zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů; citlivé údaje dle § 4 zákona č. 101/2000 Sb.
	Dotace	jméno, identifikační číslo, adresa, trvalé bydliště, doručovací adresa, e-mail, telefonní číslo – pracovní, DIČ
	Spisová služba	jméno, identifikační číslo, adresa, trvalé bydliště, doručovací adresa, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, zdravotní znevýhodnění, fotografický záznam, e-mail, telefonní číslo – soukromé i pracovní, vzdělání, příjem ze zaměstnání (mzda, plat), IČ, DIČ
	Sítové disky	jméno, identifikační číslo, adresa, trvalé bydliště, doručovací adresa, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, zdravotní znevýhodnění, fotografický záznam, e-mail, telefonní číslo – soukromé i pracovní, vzdělání, příjem ze zaměstnání (mzda, plat),
	Agendové IS, Evidence	jméno, adresa, trvalé bydliště, doručovací adresa, e-mailová adresa, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, zdravotní znevýhodnění, fotografický/video/audio záznam, e-mail, telefonní číslo – soukromé i pracovní, číslo občanského průkazu, vzdělání, příjem ze zaměstnání (mzda, plat), příjem z důchodu, kulturní profil, doklady nejvyššího dosaženého vzdělání, výpisy z rejstříku trestů,

Agenda	Typ IS	Přehled OÚ
Zdravotnictví	**Agendové IS, Evidence**	
	Agendové IS, Evidence	jméno, příjmení, titul, bydliště, místo podnikání, IČ, DIČ, bankovní spojení, funkce, datum narození, plat, odměna, doba započitatelné praxe, adresa, zaměstnavatel, e-mail, telefon, vzdělání, údaj o bezúhonnosti, zdravotní způsobilosti, datum narození
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, datum narození příp. rodné číslo, trvalý pobyt citlivé údaje: zdravotní stav údaje o jiných osobách: jméno, příjmení, odbornost, adresa místa poskytování zdravotních služeb (další dle obsahu řízení)
	Sítové disky	adresní a identifikační údaje: jméno, příjmení, datum narození příp. rodné číslo, trvalý pobyt citlivé údaje: zdravotní stav údaje o jiných osobách: jméno, příjmení, odbornost, adresa místa poskytování zdravotních služeb (další dle obsahu řízení)
Investice a majetek		
	Nespecifikované	
Finance		
	Ekonomický systém	IČ, DIČ a název firmy, sídlo, jméno podnikatele, sídlo, jména a adresa zaměstnanců, členů ZK, RK, výborů a komisí, jméno a adresa žadatelů
	Spisová služba	jméno, příjmení, titul, adresa, v případě fyzických osob podnikajících IČO, u fyzických osob nepodnikajících může být uvedeno RČ
Bezpečnost a krizové řízení		
	Technické	Popisné údaje, IP adresy, Jméno, příjmení, číslo zaměstnance/dodavatele
Dotace a projekty (evropské)		
	Dotace	titul, jméno, příjmení, datum narození, bydliště, číslo občanského průkazu, číslo cestovního pasu, funkční náplň, mzdové údaje, tel. číslo, e-mailová adresa, údaje z veřejně přístupných evidencí, IČ, DIČ
	Ekonomický systém	jméno, adresa, trvalé bydliště, doručovací adresa, pohlaví, věk, datum narození, rodné číslo, osobní stav, e-mail, telefonní číslo – soukromé i pracovní, číslo občanského průkazu, vzdělání, příjem ze zaměstnání (mzda, plat), příjem z důchodu, lokační údaje, zdravotní znevýhodnění, kulturní profil
	Kancelářský SW	jméno, příjmení, adresa, číslo OP, datum narození, telefon, email
Interní audit		
	Spisová služba	adresní a identifikační údaje: jméno, příjmení, rodné číslo, adresa trvalého bydliště, doručovací adresa jiné údaje: telefonní číslo, vzdělání, mzda, plat, e-mailový kontakt, platový výměr, výplatní lístek, mzdový list, pracovní smlouva, dohoda o provedení práce, dohoda o pracovní činnosti, pracovní náplň
	Technické	adresní a identifikační údaje: jméno, příjmení, rodné číslo, adresa trvalého bydliště, doručovací adresa jiné údaje: telefonní číslo, vzdělání, mzda, plat, e-mailový kontakt, platový výměr, výplatní lístek, mzdový list, pracovní smlouva, dohoda o provedení práce, dohoda o pracovní činnosti, pracovní náplň

Agenda	Typ IS	Přehled OÚ
	Webové portály	adresní a identifikační údaje: jméno, příjmení, rodné číslo, adresa trvalého bydliště, doručovací adresa jiné údaje: telefonní číslo, vzdělání, mzda, plat, e-mailový kontakt, platový výměr, výplatní lístek, mzdový list, pracovní smlouva, dohoda o provedení práce, dohoda o pracovní činnosti, pracovní náplň
	Sítové disky	adresní a identifikační údaje: jméno, příjmení, rodné číslo, adresa trvalého bydliště, doručovací adresa jiné údaje: telefonní číslo, vzdělání, mzda, plat, e-mailový kontakt, platový výměr, výplatní lístek, mzdový list, pracovní smlouva, dohoda o provedení práce, dohoda o pracovní činnosti, pracovní náplň

3.3.2 Právnické osoby zřizované kraji

Mapování zpracování konkrétních OÚ/COÚ v rámci činností jednotlivých agend právnických osob zřizovaných kraji je uvedeno v následujícím přehledu.

Agenda	Typ IS	Přehled OÚ
Personálně-mzdová agenda		
	Personálně-mzdový	Rozsah osobních údajů vymezený v Základních pokynech. RČ, data nar., jméno, příjmení, titul, veškerá dřívější příjmení, místo nar., bydliště, počet dětí (pokud uplatňují slevu na dani, pak i RČ dětí), státní příslušnost, zdravotní způsobilost k práci, u které ZP je pojištěncem, bankovní účet.
Úsek ekonomicko-provozní		
	Ekonomicko-provozní	faktury - jméno, příjmení doručovací adresa, IČ, pokladní doklady jméno, příjmení, číslo OP smlouvy - jméno, příjmení, adresa, IČO, číslo OP, rodné číslo, datum narození výpisy z banky - číslo bankovního účtu, příjmení, vnitřní doklady - jméno, příjmení, adresa
Knihovnické a informační služby		
	IS knihovnické a informační služby	jméno, datum narození, rodné číslo, č. OP, adresa, nepovinně: další kontaktní údaje (telefonní číslo, e-mail), ekonomická aktivita (student, pracující, důchodce)
Agenda dopravní obslužnosti		
	IS dopravní obslužnosti	Neuvedeno
Poskytování sociálních služeb		
	IS sociálních služeb	jméno a příjmení, datum narození, adresa bydliště a telefonní číslo, popř. email, pohlaví a data narození dětí, křestní jméno násilné, věk osoby Osobní údaje zaměstnanců a klientů, údaje dodavatelů
Agenda pedagogiky		
	IS pedagogika	identifikační údaje fyzické osoby včetně zákonných zástupců

Agenda	Typ IS	Přehled OÚ
Poskytování zdravotních služeb		
	IS zdravotních služeb	Jméno, zdravotní stav, (dáno legislativou)
	IS zdravotních služeb	Jméno, zdravotní stav, (dáno legislativou)

3.4 Přehled nesouladů

V rámci analýzy byla provedena identifikace níže uvedených nesouladů procesů či konkrétních postupů s požadavky vyplývajícími z jednotlivých článků GDPR. Jednotlivé nesoulady byly dále podrobně popsány a doplněny konkrétními praktickými příklady z praxe krajů nebo právnických osob zřizovaných krajem (viz Přílohy č. 5 a 6).

1. Nejasné vymezení vlastníka procesu.
2. Není stanoven účel zpracování osobních údajů.
3. Není stanoven rozsah zpracovávaných osobních údajů pro jednotlivé činnosti.
4. Není stanovena doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby.
5. Není jasně vymezen právní titul pro zpracování osobních údajů.
6. Souhlasy se zpracováním osobních údajů nejsou dány jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se ho týkají.
7. Subjekt údajů není informován o zpracování osobních údajů.
8. Nejsou stanovena jasná pravidla pro přístupová oprávnění.
9. Není vedena evidence zpracovávaní osobních údajů.
10. Chybí pravidla pro případy uplatnění práv subjektů údajů podle čl. 15–22 GDPR.
11. Absence kontrolních mechanismů.
12. Zpracování osobních údajů, které je prováděno zpracovatelem na základě uzavřené smlouvy se správcem či na základě jiného právního aktu nesplňuje požadované náležitosti obsahu těchto smluv či jiných aktů.
13. V případě, že správce poskytuje osobní údaje dalším osobám (příjemcům) na základě uzavřené smlouvy, není ve smlouvě dostatečně řešena ochrana takto poskytnutých osobních údajů.
14. Chybí systém pro ohlašování porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů.
15. Chybí systém pro oznamování porušení zabezpečení osobních údajů subjektům údajů.
16. Chybí systém pro vyhodnocování rizik souvisejících se zpracováním osobních údajů.

3.5 Přehled systémů, rizika

Na základě zpracované analýzy lze konstatovat, že dílčí části systémů řízení bezpečnosti informací jsou v organizacích přítomné, ale nejsou ucelené tak, aby plně pokryly potřeby GDPR. Využívané části bezpečnosti informací pozitivním způsobem ovlivňují celkovou bezpečnost OÚ/COÚ.

Organizace nemají zpracovanou analýzu rizik s ohledem na dopad na SÚ. Analýza rizik je povinný dokument, na jehož základě musí být posuzována prováděná bezpečnostní opatření. Dílčí bezpečnostní opatření, která nenavazují na analýzu rizik, nelze považovat jako dostatečná v kontextu povinností dle GDPR. Je tedy nutné připravit analýzu rizik, na jejím základě posoudit současná bezpečnostní opatření a v případě nedostatků navrhnout nápravné kroky vedoucí k souladu s GDPR.

3.5.1 Kraje

Obrázek níže interpretuje soulad současných zavedených technických opatření v návaznosti na GDPR. Vyplývá z toho, že IT systémy krajů jsou v průměru zabezpečené (v souladu) dle obecné best practice, která ale přímo nereflektuje požadavky na zabezpečení OÚ/COÚ dle GDPR. Z důvodu neexistence konkrétní analýzy rizik v organizacích dle článku 32, bod 1 GDPR není možné posoudit, zda tato bezpečnostní opatření jsou relevantní a dostatečná pro ochranu OÚ/COÚ. Po provedení analýzy rizik je nutné znovu posoudit bezpečnostní opatření, která v některých případech mohou být dostatečná nebo naopak bude nutné bezpečnostní opatření rozšířit.

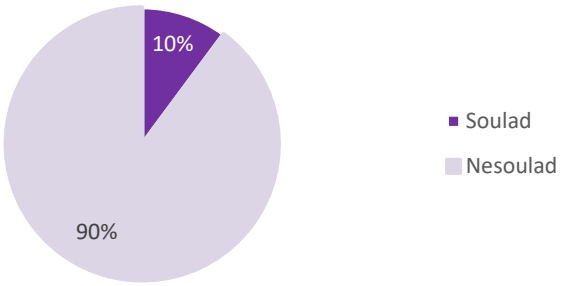
Detailní přehled je uveden v kapitole Příloha 3 – Přehled systémů (Kraje), list Přehled typů systémů.

Souhrnná analýza rizik byla zpracována na základě zjištěných informací v rámci dotazníkového šetření. Výsledná míra rizika je stanovena jako úroveň dopadu na SÚ a pravděpodobnost hrozby. V případě, že je riziko vysoké, bude nutné provést DPIA, viz kapitola 4.3 Povinnost provádění posouzení vlivu na ochranu osobních údajů (DPIA). Toto se může týkat zejména následujících agend:

- Sociální věci,
- Zdravotnictví,
- Bezpečnost a krizové řízení.

3.5.2 Právnické osoby zřizované kraji

Obrázek níže interpretuje soulad současných zavedených technických opatření v návaznosti na GDPR. Vyplývá z toho, že IT systémy právnických osob zřizovaných kraji jsou podprůměrně zabezpečené (v souladu) dle obecné best practice, která ale přímo nereflektuje požadavky na zabezpečení OÚ/COÚ dle GDPR. Z důvodu neexistence konkrétní analýzy rizik v organizacích dle článku 32, bod 1 GDPR není možné posoudit, zda tato bezpečnostní opatření jsou relevantní a dostatečná pro ochranu OÚ/COÚ. Po provedení analýzy rizik je nutné znovu posoudit bezpečnostní opatření, která v některých případech mohou být dostatečná nebo naopak bude nutné bezpečnostní opatření rozšířit.



Detailní přehled je uveden v kapitole Příloha 4 – Přehled systémů (Právnické osoby zřizované kraji), list Přehled typů systémů.

V případě, že je riziko vysoké, bude nutné provést DPIA, viz kapitola 4.3 Povinnost provádění posouzení vlivu na ochranu osobních údajů (DPIA). Toto se může týkat zejména následujících agend:

- Poskytování zdravotních služeb,
- Poskytování sociálních služeb.

4 Doporučení

Níže uvedené závěry/doporučení/mechanismy vychází ze systémové analýzy provedené na vzorku 3 krajů a 8 právnických osob zřizovaných kraji. Míru dopadu výše uvedených závěrů/doporučení/mechanismů tudíž musí posoudit každý správce osobních údajů ve smyslu čl. 4 odst. 7 GDPR, který vykonává činnosti spadající do věcné působnosti GDPR (čl. 2 odst. 1 GDPR), případ od případu a dle konkrétních okolností, zejména se zohledněním stanovených účelů, podmínek zpracování osobních údajů a úrovně zavedených organizačních a technických opatření. Odpovědný za zpracování osobních údajů v souladu s GDPR je totiž vždy správce, přičemž správce zároveň musí být schopen toto dodržení souladu doložit (čl. 5 odst. 2 a čl. 24 odst. 1 GDPR)

4.1 Organizační, procesní a právní doporučení

V rámci provedené analýzy byly identifikovány nesoulady s požadavky GDPR. K jednotlivým nesouladům byla doporučena následující organizační, procesní a právní opatření. Tato opatření byla dále podrobně popsána a opatřena prioritizací jejich implementace (viz přílohy 5 a 6*)*.

1. Provedení revize interních předpisů (zejména za účelem vymezení rolí a odpovědností ve vztahu ke každé činnosti vykonávané v rámci organizace).
2. Stanovení účelů zpracování a rozsahu zpracovávaných osobních údajů.
3. Kontrola přesnosti zpracovávaných osobních údajů.
4. Kontrola doby uložení osobních údajů.
5. Provedení auditu právních titulů ke zpracování.
6. Revize stávajících souhlasů.
7. Zavedení systému záznamů o udělených souhlasech.
8. Zpracování či revize dokumentu s informacemi pro subjekt údajů.
9. Vedení záznamu o splnění informační povinnosti.
10. Vedení záznamů o činnostech zpracování.
11. Zavedení mechanismů za účelem výkonu práv subjektů údajů.
12. Jmenovaní pověřence pro ochranu osobních údajů.
13. Stanovení podmínek zapojení zpracovatele (např. ve vnitřních předpisech).
14. Zpracování vzorové smluvní doložky k ochraně osobních údajů.
15. Zavedení postupu pro ohlášení/oznámení porušení zabezpečení osobních údajů.
16. Posouzení rizik pro práva a svobody fyzických osob.
17. Dokumentace případů porušení zabezpečení osobních údajů.
18. Analýza rizik a hodnocení rizik zpracování osobních údajů.
19. Provedení posouzení vlivu na ochranu osobních údajů.

4.2 Technická opatření

Přehled technických opatření k zabezpečení ochrany a zpracování OÚ/COÚ, zejména pak takových, která musí organizace provést ve svých zákaznických, zaměstnaneckých nebo jiných systémech, v nichž dochází ke zpracování osobních údajů, aby byly v souladu s GDPR, následuje v navazujících kapitolách.

4.2.1 Kraje

Doporučení pro jednotlivé systémy byla volena s ohledem na velikost organizace, stav zabezpečení v organizaci, best practice, náklady na provedení v souvislosti s rizikem a povahu osobních údajů, které mají být chráněny. Tato opatření reflektují výsledek risk analýzy a požadavky Nařízení.

Následující doporučení platí pro většinu systémů dle zpracované analýzy:

1. vedení auditních záznamů (logů) a napojení na centrální monitoring,
2. rozšíření disaster recovery plánu pro veškeré systémy,
3. zajištění přenosu dat výhradně šifrovanou komunikací,
4. zavedení pravidelného testování disaster recovery plánů.

Vedení auditních logů a napojení na centrální monitoring (SIEM/SOC) slouží k identifikaci incidentů, které je nezbytné při vyšetřování zneužití OÚ/COÚ.

Dalším doporučením je rozšíření disaster recovery plánu pro veškeré systémy. V současné době má tyto plány zpracovány polovina systémů. S těmito plány souvisí i jejich pravidelné testování, aby došlo k ověření, že v případě incidentu/havárie je reálné tyto systémy obnovit do provozu s ohledem na integritu dat. Mezi disaster recovery plán patří i pravidelné testování obnovy systému ze zálohy, které je prováděno pouze u několika systémů, jak vyplývá ze zpracované analýzy. Testování je vhodné provádět nejen jednorázově, ale pravidelně nebo alespoň při každé změně systému s dopadem na bezpečnost. Zároveň je nutné při zjištění hrozeb přijmout vhodná opatření k zamezení vzniku zjištěných hrozeb.

Zajištění přenosu OÚ/COÚ výhradně šifrovanou komunikací zamezí odcizení údajů pomocí odposlouchávání komunikace.

Přehled všech nesouladů a doporučení pro kraje v oblasti technických doporučení je uveden v kapitole Příloha 5 – Přehled nesouladů a doporučení (Kraje).

4.2.2 Právnické osoby zřizované kraji

Doporučení pro jednotlivé systémy byla volena s ohledem na velikost organizace, stav zabezpečení v organizaci, best practice, náklady na provedení v souvislosti s rizikem a povahu osobních údajů, které mají být chráněny. Tato opatření reflektují výsledek risk analýzy a požadavky Nařízení.

Následující doporučení platí pro většinu systémů dle zpracované analýzy:

1. vedení auditních záznamů (logů),

2. rozšíření disaster recovery plánu pro veškeré systémy,
3. zavedení pravidelného testování obnovy ze zálohy,
4. zavedení pravidelného vyhodnocování incidentů,
5. zavedení pravidelného testování disaster recovery plánů.

Vedení auditních logů slouží k identifikaci incidentů, které je nezbytné při vyšetřování zneužití OÚ/COÚ.

Disaster recovery plány má, dle provedené analýzy, v současné době zpracovány polovina systémů. S těmito plány souvisí i jejich pravidelné testování, aby došlo k ověření, že v případě incidentu/havárie je reálné tyto systémy obnovit do provozu s ohledem na integritu dat. Mezi disaster recovery plán patří i pravidelné testování obnovy systému ze zálohy, které není prováděno u žádného ze systémů.

V současné době testování obnovy ze zálohy probíhá pouze u malého počtu systémů. Testování obnovy ze zálohy by mělo být zavedeno v rámci disaster recovery plánu, které jsou ve společnosti zavedeny pro většinu systémů.

Zavedení pravidelného vyhodnocování incidentů je nezbytný předpoklad pro kontinuální zvyšování zabezpečení OU. V současné době probíhá vyhodnocování incidentů pouze pro polovinu systémů.

Pro prevenci před porušením dostupnosti a integrity je vhodné zavést pravidelné testování disaster recovery plánů. Testování je vhodné provádět nejen jednorázově, ale pravidelně nebo alespoň při každé změně systému s dopadem na bezpečnost. Zároveň je nutné při zjištění hrozeb přijmout vhodná opatření k zamezení vzniku zjištěných hrozeb.

Přehled nesouladů a doporučení pro právnické osoby zřizované kraji v oblasti technických doporučení je uveden v kapitole Příloha 6 – Přehled nesouladů a doporučení (Právnické osoby zřizované kraji).

4.3 Povinnost provádění posouzení vlivu na ochranu osobních údajů (DPIA)

Podle čl. 35 odst. 1 GDPR je správce povinen v případě, že 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, provést před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů (dále jen „**DPIA**“). Významné je pro tyto účely mj. též hledisko, zda se činnost zpracování dotýká zranitelných subjektů údajů.

Povinnost provedení DPIA se vztahuje též na stávající operace zpracování, u nichž došlo ke změně rizik s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování.

Výjimku z této povinnosti představuje zpracování prováděné na základě čl. 6 odst. 1 písm. c) nebo e) GDPR, pokud má zpracování právní základ v právu Unie nebo právu ČR a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu

osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu.

Podle názoru pracovní skupiny WP29 se provedení DPIA nevyžaduje ani u těch operací zpracování, které prošly kontrolou dozorového úřadu podle článku 20 směrnice 96/46/ES a které jsou prováděny způsobem, jenž se od předchozí kontroly nezměnil. Článek 20 směrnice 96/46/ES se do vnitrostátní právní úpravy promítl v ust. § 16 zákona o ochraně osobních údajů, a to zakotvením tzv. oznamovací povinnosti.

Dle výše uvedeného proto lze dovozovat, že povinnost provést DPIA se bude vztahovat též na operace zpracování, s nimiž bylo započato ještě před tím, než bude GDPR přímo použitelné (tj. před 25. 5. 2018), pokud došlo ke změně rizik. Provedení DPIA se nebude vyžadovat v případech, kdy zpracování je nezbytné a) pro splnění zákonem uložené povinnosti, nebo b) pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, a pokud současně bylo provedeno posouzení v rámci legislativního procesu. Provedení DPIA nebude vyžadováno ani v případech, kdy správce dle § 16 zákona o ochraně osobních údajů splnil vůči dozorovému úřadu oznamovací povinnost, za předpokladu, že nedošlo ke změně ve způsobu provádění předmětných operací zpracování.

Návrh zákona o zpracování osobních údajů v § 9 vymezuje výjimku z povinnosti provedení DPIA následovně: „*Před zahájením zpracování osobních údajů, které je upravené právním předpisem, není nutno provádět posouzení vlivu takového zpracování na ochranu osobních údajů.*“ Uvedené však nezbytně nutně předpokládá, že v rámci legislativního procesu u konkrétní právní úpravy bylo provedeno hodnocení dopadů regulace (tzv. RIA), s tím, že zároveň bude nutné posuzovat míru provedeného hodnocení ve vztahu k ochraně osobních údajů vždy v rámci konkrétního případu. V kontextu navrhované výjimky se proto předpokládá, že problematika DPIA bude dopadat pouze na činnosti vykonávané v rámci samostatné působnosti krajů.[24]

Výše uvedené závěry však vycházejí ze současných výkladových stanovisek k GDPR, aplikační praxe může přinést v tomto směru zcela odlišný názor.

I přes výše uvedené se každému správci údajů v každém případě doporučuje v rámci své organizace provést analýzu rizik a následně přijmout relevantní vhodná a účinná opatření za účelem doložení souladu jeho postupů s GDPR.

4.4 Přehled právních titulů dle jednotlivých agend

Přehled právních titulů dle čl. 6 odst. 1 GDPR ke zpracování osobních údajů ve vztahu k vykonávaným činnostem, při nichž dochází ke zpracování osobních údajů, je uveden v přílohách č. 7 a 8. S ohledem na povahu činnosti analyzovaných organizací je zpracování osobních údajů nejčastěji

[24] Uvedený závěr koresponduje rovněž s úvahou autora textu, že v případě realizace činností v rámci výkonu přenesené působnosti budou kraje zásadně vystupovat v roli zpracovatele (viz kapitola 1.3.2 Pro koho je tento dokument určen?), neboť povinnost provedení DPIA dopadá pouze na správce, nikoli na zpracovatele osobních údajů.

prováděno na základě právního titulu splnění právní povinnosti (viz čl. 6 odst. 1 písm. c) GDPR). K jednotlivým činnostem byla rovněž identifikována relevantní právní úprava.

4.5 Pověřenec pro ochranu osobních údajů

Nařízení zavádí plošně pro všechny členské státy EU nový institut pověřence pro ochranu osobních údajů (dále také jako „**pověřenec**“).

Role pověřence spočívá zejména v monitorování souladu postupů správců[25] a zpracovatelů[26] osobních údajů s Nařízením a poskytování poradenství a informací o jejich povinnostech souvisejících s ochranou osobních údajů. Správce nebo zpracovatel má povinnost zapojit pověřence do všech záležitostí souvisejících s ochranou osobních údajů a podporovat ho při plnění jeho úkolů a povinností. Nařízení rovněž zakotvuje požadavek nezávislosti výkonu funkce pověřence. Pověřenec tedy není jen pouhým řadovým zaměstnancem správce, který má na starosti ochranu osobních údajů. Požadavky na osobu pověřence a vymezení postavení pověřence v rámci organizační struktury správce nebo zpracovatele, jeho úkolů, povinností a odpovědností jsou podrobněji rozebrány níže.

Pověřenec je specifickým subjektem, jehož musí jmenovat správci a zpracovatelé osobních údajů stanovení v čl. 37 odst. 1 Nařízení. Správce a zpracovatel jmenují pověřence v každém případě, kdy:

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů[27]; nebo
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování COÚ uvedených v čl. 9 Nařízení a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 Nařízení.

Každý správce a zpracovatel by měl vždy zvážit a interně vyhodnotit, zda spadá do některé z výše popsaných skupin zpracování osobních údajů, u nichž je jmenování pověřence povinné.

4.5.1 Povinné jmenování pověřence podle čl. 37 odst. 1 písm. a) Nařízení

Čl. 37 odst. 1 písm. a) Nařízení stanoví povinnost jmenovat pověřence v případě, kdy zpracování provádí orgán veřejné moci nebo veřejný subjekt. Tyto pojmy nejsou v Nařízení přímo definovány, jejich bližší vymezení poskytuje např. výkladové stanovisko WP 29[28] a také další nezávazné dokumenty v podobě komentářů k Nařízení. Orgány veřejné moci a veřejnými subjekty jsou dle výkladového stanoviska WP 29 národní, regionální a místní úřady, které plní úkoly ve veřejném zájmu a vykonávají veřejnou moc. Obecně se tak orgánem veřejné moci rozumí orgán, který reprezentuje veřejnou moc a je ze zákona oprávněn autoritativně rozhodovat o právech a

[25] Ve smyslu čl. 4 odst. 7) Nařízení.
[26] Ve smyslu čl. 4 odst. 8) Nařízení.
[27] Ve smyslu čl. 4 odst. 1) Nařízení.
[28] Viz Pracovní skupina podle čl. 29, Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev.01.

povinnostech fyzických a právnických osob nebo jinak zasahovat do jejich právní sféry. Veřejným subjektem bude především subjekt zřízený zákonem nebo na základě zákona, který plní zákonem stanovené úkoly ve veřejném zájmu.

Pojmovým znakem, který bude odůvodňovat jmenování pověřence podle čl. 37 odst. 1 písm. a) Nařízení, bude především skutečnost, že daný subjekt autoritativně rozhoduje o právech a povinnostech fyzických osob. Vyšší územní samosprávné celky (dále také jako „**kraj**“) jsou tak ve smyslu čl. 37 odst. 1 písm. a) Nařízení orgány veřejné moci, které jsou povinny pověřence jmenovat.

Výše rozebrané kompetence mohou být uloženy také jiným fyzickým nebo právnickým osobám, které se řídí veřejným nebo soukromým právem v oblastech specifikovaných zvláštními právními předpisy (např. veřejná doprava, zásobování energiemi, veřejné bydlení atd.). Výkladové stanovisko WP 29 doporučuje, aby soukromé organizace (např. některé příspěvkové organizace) vykonávající úkol ve veřejném zájmu pověřence jmenovaly. Nicméně, důvodová zpráva k návrhu zákona o zpracování osobních údajů k tomu uvádí, že definice orgánu veřejné moci nebo veřejného subjektu záměrně nedopadá např. na příspěvkové organizace či jiné pomocné instituce, protože v případech, kdy taková instituce provádí zpracování, jež vyžaduje nasazení pověřence, bude pokryta ustanoveními čl. 37 odst. 1 písm. b) nebo c) Nařízení. Naopak pokud tento subjekt takové zpracování neprovádí, ani není ve zvláštním vztahu k subjektům údajů, bylo by zavádění pověřenců dle důvodové zprávy zbytečnou administrativní zátěží.

4.5.2 Povinné jmenování pověřence podle čl. 37 odst. 1 písm. b) a c) Nařízení

K jednotlivým podmínkám stanovených v čl. 37 odst. 1 písm. b) a c) Nařízení uvádíme následující:

4.5.2.1 Hlavní činnost

Prvním nezbytným kritériem pro určení povinnosti jmenovat pověřence dle čl. 37 odst. 1 písm. b) a c) Nařízení je hlavní činnost správce nebo zpracovatele. Zpracování musí být vlastní (imanentní) činností správce nebo zpracovatele. Hlavní činnost lze chápat jako činnost, kterou správce nebo zpracovatel provádí za účelem provádění svých základních činností či stanovených cílů a která je s těmito činnostmi nebo cíli neoddělitelně spojena. Jako příklad je možné uvést nemocnici, jako poskytovatele zdravotních služeb, u které je hlavní činností poskytování zdravotních služeb, s čímž je neoddělitelně spjato zpracování osobních údajů (zejm. COÚ).

4.5.2.2 Rozsáhlé zpracování osobních údajů

Dalším definičním znakem dle čl. 37 odst. 1 písm. b) a c) Nařízení je rozsáhlost zpracování osobních údajů. Pojem rozsáhlého zpracování osobních údajů není v Nařízení definován. Dopad tohoto kritéria na povinnost jmenovat pověřence tak bude nutné posuzovat případ od případu. Výkladové stanovisko WP 29 při tomto posuzování doporučuje vzít v úvahu několik faktorů:

- počet dotčených subjektů údajů,
- objem dat a/nebo rozsah různých datových položek,
- dobu trvání nebo nepřetržitost zpracování,

- územní rozsah zpracování.

Jako příklad rozsáhlého zpracování je uváděno zpracování COÚ o pacientech v rámci činnosti nemocnice nebo zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy.

4.5.2.3 Pravidelné a systematické monitorování (čl. 37 odst. 1 písm. b) Nařízení)

Další podmínkou, týkající se pouze čl. 37 odst. 1 písm. b) Nařízení, je pravidelné a systematické monitorování subjektů údajů. Pojem pravidelné a systematické monitorování rovněž není v Nařízení definován. Musí se jednat o průběžné monitorování subjektů údajů nebo monitorování opakující se v pravidelných intervalech, přičemž toto pravidelné monitorování se musí opakovat podle určitého, předem organizovaného systému.[29]

Dle Nařízení se jedná především o všechny formy sledování a profilování na internetu.[30] Za další formy monitorování chování subjektů údajů lze označit např. sledování polohy na základě lokalizačních údajů nebo monitorování prostor pomocí kamerových systémů.

4.5.2.4 Zvláštní kategorie osobních údajů a osobní údaje týkající se rozsudků v trestních věcech a trestných činů (čl. 37 odst. 1 písm. c) Nařízení)

Další podmínka, týkající se pouze čl. 37 odst. 1 písm. c) Nařízení, spočívá v požadavku zpracovávání zvláštních kategorií osobních údajů (viz čl. 9 Nařízení) a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů (viz čl. 10 Nařízení). V tomto kontextu je třeba upozornit na skutečnost, že ke vzniku povinnosti jmenovat pověřence, samozřejmě za předpokladu splnění dalších podmínek stanovených tímto ustanovením, stačí, že správce nebo zpracovatel zpracovává buď zvláštní kategorie osobních údajů, nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů.

4.5.3 Podřízené organizace kraje a povinnost jmenovat pověřence

Povinnost jmenovat pověřence se bude vztahovat vždy pouze na ty podřízené organizace, které mají právní subjektivitu ve smyslu zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů. Na ostatní podřízené organizace, které jsou součástí organizační struktury kraje, resp. organizačními složkami kraje, tato povinnost nedopadá, ale bude se vztahovat pouze na kraj, jehož součástí daná organizace je.

V případě podřízených organizací s právní subjektivitou bude vždy nutné zvážit, jestli je naplněna některá z podmínek stanovených čl. 37 odst. 1 Nařízení. Povinnost jmenovat pověřence tak budou mít zejména poskytovatelé zdravotních služeb, jejichž činnost spočívá v rozsáhlém zpracování

[29] Viz Pracovní skupina podle čl. 29, Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev.01.
[30] Viz bod 24 recitálu k Nařízení.

zvláštních kategorií osobních údajů, tedy například nemocnice[31], případně poskytovatelé sociálních služeb, jako jsou např. domovy pro osoby s chronickým duševním onemocněním nebo se závislostí na návykových látkách nebo zařízení pro osoby se zdravotním postižením. Povinnost jmenovat pověřence budou mít rovněž poskytovatelé sociálních služeb, kteří provádí rozsáhlé zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. Povinnost jmenovat pověřence se bude vztahovat také na školy a školská zařízení, které jsou považovány za orgány veřejné moci ve smyslu čl. 37 odst. 1 písm. a) Nařízení.[32]

4.5.4 Doporučení k osobě a organizačnímu začlenění pověřence

4.5.4.1 Osoba pověřence

4.5.4.1.1 Odborné požadavky na osobu pověřence

Pověřenec musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů, a na základě své schopnosti plnit úkoly stanovené v čl. 39 Nařízení. Mělo by se tedy jednat o osobu znalou postupů týkajících se ochrany osobních údajů, ideálně s praxí v této oblasti. Otázka formálního vzdělání či certifikace pověřenců však není nijak upravena, žádný certifikát, ani konkrétní vysokoškolský titul tedy není pro výkon činnosti pověřence povinný.

Požadovaná úroveň odborných znalostí není Nařízením nikterak konkretizována. Tento požadavek by měl být určen zejména se zohledněním operací zpracování osobních údajů prováděných správcem nebo zpracovatelem dle vyžadované míry ochrany osobních údajů, a též by měl být úměrný citlivosti, složitosti a množství osobních údajů, které správce či zpracovatel zpracovává. Pověřenec by měl být vybrán pečlivě a s náležitým zvážením specifických otázek ochrany osobních údajů, které správce nebo zpracovatel řeší.

Zejména v oblasti veřejné správy by pověřenec také měl mít dostatečnou znalost prováděných operací zpracování, stejně jako řízení informačních systémů[33], řízení procesů[34], bezpečnosti dat (jak kybernetické bezpečnosti, tak také bezpečnosti fyzické, osobní údaje je třeba chránit i v analogové podobě) a správcových nebo zpracovatelových potřeb v oblasti ochrany osobních údajů. Navíc by měl pověřenec nepochybně dobře znát administrativní pravidla a postupy uplatňované při činnosti správce nebo zpracovatele.

---

[31] Jako příklad zpracování, která jsou rozsáhlá, uvádí výkladové stanovisko WP29 zpracování údajů o pacientech v rámci běžné činnosti nemocnice, naproti tomu jako zpracování, které není rozsáhlé, označuje zpracování údajů o pacientech jednotlivým lékařem.

[32] Viz *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství*, vydaná Ministerstvem školství, mládeže a tělovýchovy, a dále *Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí,* vypracovaného Ministerstvem vnitra.

[33] Viz normy řady ISO 27000.

[34] Viz normy řady ISO 9000.

4.5.4.1.2 Postavení a odpovědnost pověřence

Pověřenec nenese osobní odpovědnost za nedodržení pravidel stanovených Nařízením. Tuto odpovědnost má přímo správce osobních údajů.[35] Dle čl. 24 odst. 1 Nařízení spočívá tato odpovědnost zejména v tom, že správce je povinen dodržovat všechny povinnosti plynoucí z Nařízení, přičemž za tímto účelem musí zavést vhodná technická a organizační opatření, a zároveň musí být schopen dodržení tohoto souladu doložit.

Pověřenec by měl v rámci správce nebo zpracovatele vždy zastávat svou funkci a plnit své povinnosti a úkoly nezávislým způsobem. Správce nebo zpracovatel zajistí, aby pověřenec nedostával žádné pokyny týkající se výkonu jeho úkolů stanovených v Nařízení.[36]

Zajištění souladu postupů správce nebo zpracovatele s Nařízením není odpovědností pověřence, proto pokud správce nebo zpracovatel postupuje v rozporu s názorem pověřence a takový postup povede k závěru o nesouladu jeho postupu s Nařízením, není v kompetencích pověřence v tom správci nebo zpracovateli bránit. Pověřenec by ale měl vždy mít možnost vyjádřit svůj názor a správce nebo zpracovatel by měl být vždy schopen zdůvodnit, proč názor pověřence nebude respektovat.[37]

Pověřenec dle čl. 38 odst. 3 Nařízení nesmí být v souvislosti s plněním svých úkolů propuštěn ani sankcionován, analogicky by z těchto důvodů neměla být vypovězena ani smlouva o poskytování služeb uzavřená s pověřencem, který vykonává svou funkci mimo pracovní poměr (dále také jako „**externí pověřenec**"). Tato zvýšená ochrana pověřence však nevylučuje nárok správce nebo zpracovatele na náhradu škody způsobené mu pověřencem (to platí jistě při provádění činností nevázaných přímo na ochranu osobních údajů). Správce nebo zpracovatel však nemůže po pověřenci požadovat náhradu škody v případě, kdy pověřenec poukáže na nesoulad postupů s Nařízením. V případě, že pověřenec vykonává svou funkci v rámci pracovněprávního vztahu, je možné pověřence propustit nebo sankcionovat pouze dle pravidel stanovených zákoníkem práce[38], nikoli však v souvislosti s plněním úkolů pověřence dle Nařízení.

4.5.4.1.3 Povinnost mlčenlivosti pověřence

Pověřenec je v souvislosti s výkonem svých úkolů vázán povinností mlčenlivosti, resp. povinností zachovávat tajemství nebo důvěrnost (čl. 38 odst. 5 Nařízení). Uvedené platí zejména v souvislosti se skutečností, že se pověřenec při výkonu své funkce může setkat s množstvím důvěrných informací.

---

[35] Viz NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR/Obecné nařízení o ochraně osobních údajů: praktický komentář. 1. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3.

[36] Viz čl. 39 Nařízení.

[37] Viz NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR/Obecné nařízení o ochraně osobních údajů: praktický komentář. 1. Praha: Wolters Kluwer ČR, 2017. ISBN 978-80-7552-765-3.

[38] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

4.5.4.2 Organizační začlenění pověřence

Dle Nařízení je správce nebo zpracovatel povinen zajistit, aby byl pověřenec náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Je důležité, aby byl pověřenec brán jako diskuzní partner v rámci správce nebo zpracovatele a měl přístup do pracovních skupin správce nebo zpracovatele, zabývajících se zpracováním osobních údajů. WP 29 ve svém výkladovém stanovisku výslovně doporučuje, aby byl pověřenec součástí příslušných pracovních skupin.

Nařízení rovněž požaduje, aby byl pověřenec přímo podřízen vrcholným řídícím pracovníkům správce nebo zpracovatele, z čehož a contrario vyplývá, že pověřenec nemůže být například hejtmanem kraje, neboť ten je takovým řídícím pracovníkem. Pověřenec však musí mít zajištěn přímý přístup k vedení správce nebo zpracovatele (tj. v případě kraje k řediteli krajského úřadu nebo přímo k hejtmanovi).

4.5.4.2.1 Střet zájmů

Výčet úkolů a povinností pověřence dle Nařízení není taxativní, pověřenec tedy na základě dohody se správcem či zpracovatelem může plnit i jiné úkoly a povinnosti, které nejsou výslovně Nařízením stanoveny, vždy však při dodržení principu zákazu střetu zájmů.

Výkon činnosti pověřence je však omezen tím, že pověřenec nemůže zastávat pozici, na které by stanovoval účely nebo prostředky zpracování osobních údajů.[39]

Za typicky „konfliktní" jsou považovány pozice vykonávané v rámci vyššího managementu, tedy například pozice výkonného ředitele, finančního ředitele, vedoucího IT oddělení apod.

Pozicemi ve střetu zájmů mohou být ale rovněž pozice na nižším stupni organizační struktury správce nebo zpracovatele za předpokladu, že i na takovémto místě dochází v rámci výkonu kompetencí k rozhodování o účelech nebo prostředcích zpracování osobních údajů. Jednoduše řečeno, osoby ve střetu zájmů budou ty, které se podílejí jak na koncipování, tak realizaci projektů zahrnujících činnosti v souvislosti se zpracováním osobních údajů.

Na základě výše uvedeného lze tedy dovodit, že pověřenec by se ani neměl podílet na činnosti, v rámci níž by určoval účely nebo prostředky zpracování osobních údajů.

Pro bližší představu, v případě, že by pověřencem byla ustanovena osoba v postavení právníka správce, neměla by tato osoba v rámci výkonu své činnosti zejména sepisovat smlouvy, pojistné podmínky nebo se podílet na dalších podobných činnostech. Naopak by se neměl pověřenec ocitnout ve střetu zájmů při zastupování správce nebo zpracovatele v řízení před soudy nebo správními orgány, pokud se tato řízení netýkají přímo ochrany osobních údajů.

[39] Viz Pracovní skupina podle čl. 29, Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev.01.

4.5.4.2.2 Interní a externí pověřenec

Pověřenec může být zaměstnancem správce nebo zpracovatele (tzv. interní pověřenec), nebo může jednotlivé úkoly plnit na základě smlouvy o poskytování služeb[40] (tzv. externí pověřenec). Externě může plnění povinností pověřence zajišťovat také právnická osoba, avšak jen tehdy, pokud bude fakticky tuto činnost vykonávat fyzická osoba, která bude splňovat požadavky kladené Nařízením na osobu pověřence.

Lze doporučit, v souladu se zněním výkladového stanoviska WP 29, pro případy, kdy bude pověřenec ustanoven interně jako zaměstnanec, aby správce nebo zpracovatel provedl přímé interní označení konkrétních pracovních pozic nekompatibilních s výkonem funkce pověřence. Je tedy třeba zvážit náplň práce zaměstnanců na jednotlivých pozicích a míru možného střetu zájmů těchto pozic s výkonem funkce pověřence. V případě externího pověřence bude vhodné určit činnosti, které by zapříčinily střet zájmů, ve smlouvě o poskytování služeb.

Interní pověřenec – výhody[41]

- Pověřenec v pracovním poměru je v každodenním bezprostředním kontaktu se svým zaměstnavatelem, zná tedy dobře provoz a činnosti správce nebo zpracovatele.
- Interní pověřenec dokáže okamžitě reagovat na zjištěné nedostatky v oblasti ochrany osobních údajů, neboť zná detailně strukturu svého zaměstnavatele, a zároveň je ve většině případů přítomen přímo na pracovišti.
- Zaměstnanec je seznámen s detaily činností zaměstnavatele, které mohou externímu subjektu uniknout.

Externí pověřenec – výhody[42]

- Vzhledem ke skutečnosti, že se na externího pověřence nevztahují omezení vyplývající ze zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, a není součástí vnitřní hierarchické struktury správce nebo zpracovatele, lze lépe zajistit jeho nezávislost a naplnění principu zákazu střetu zájmů.
- Externí pověřenec může přinést nový pohled na situaci uvnitř správce nebo zpracovatele.
- Externí pověřenec není nijak, s výjimkou uzavřené smlouvy, omezen v souvislosti s jeho odpovědností za případnou škodu způsobenou správci nebo zpracovateli, na rozdíl od interního pověřence, který jako zaměstnanec správce bude odpovídat za škodu způsobenou zaměstnavateli pouze v omezeném rozsahu dle zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů.
- Externí pověřenec může mít k dispozici širší odborné zázemí a v případě nenadálých událostí může být jednodušeji zastupitelný. V případě, že externím pověřencem bude jmenována

[40] Půjde o nepojmenovanou soukromoprávní smlouvu mezi správcem a pověřencem ve smyslu ust. § 1746 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
[41] Srov. viz NAVRÁTIL, J. a kol. GDPR pro praxi. Plzeň: Aleš Čeněk, 2018, 339 s. ISBN 978-80-7380-689-7.
[42] Srov. viz NAVRÁTIL, J. a kol. GDPR pro praxi. Plzeň: Aleš Čeněk, 2018, 339 s. ISBN 978-80-7380-689-7.

právnická osoba, je možné jednoduše nahradit konkrétní osobu, která je v rámci právnické osoby odpovědná za výkon úkolů pověřence.

4.5.4.2.3 Společný pověřenec

Nařízení také umožňuje, aby pro několik orgánů veřejné moci či veřejných subjektů byl jmenován jediný pověřenec. V takovém případě však musí být zohledněna organizační struktura a velikost jednotlivých správců nebo zpracovatelů, neboť každý správce nebo zpracovatel je odpovědný za zajištění toho, že tento jediný pověřenec bude vůči němu plnit své úkoly efektivně. Pověřenec současně musí být schopen splňovat podmínku dostupnosti pro všechny subjekty údajů, jejichž osobní údaje jednotliví správci nebo zpracovatelé zpracovávají.

4.5.4.3 Doporučení

- Správce nebo zpracovatel musí dostatečným způsobem zajistit nezávislost postavení pověřence a výkonu jeho funkce.
- Pověřenec by neměl stanovovat účely nebo prostředky zpracování osobních údajů, v rámci správce nebo zpracovatele by tak neměl disponovat rozhodovacími pravomocemi nad rámec svých úkolů dle čl. 39 Nařízení.
- V případě, že pověřenec bude ustanoven interně jako zaměstnanec správce nebo zpracovatele, doporučujeme správci provést přímé označení konkrétních pracovních pozic nekompatibilních s výkonem funkce pověřence. V případě externího pověřence bude vhodné určit činnosti, které by zapříčinily střet zájmů, ve smlouvě o poskytování služeb.
- Vzhledem k doposud ne zcela jasnému výkladu principu zákazu střetu zájmů zakotvenému v Nařízení, který bude nejspíše ujasněn až příslušnou rozhodovací praxí, doporučujeme ustanovit pověřence jako nezávislého kontrolora ochrany osobních údajů, který bude oprávněn vyřizovat podněty a stížnosti subjektů údajů na výkon jejich práv dle čl. 15 – 22 Nařízení, přičemž prostřednictvím vyřizování těchto podnětů a stížností bude provádět kontrolu postupů správce ve věcech ochrany osobních údajů, a dále bude zajišťovat roli konzultanta a poradce, přičemž tyto kompetence pověřence musí být striktně odděleny od výkonných činností správce.
- Zároveň doporučujeme vytvořit metodické pracoviště, které by centrálně zaštiťovalo činnosti jednotlivých osob pracujících s osobními údaji a zajišťujících výkon práv subjektů údajů – pověřenec nemá být součástí tohoto metodického pracoviště, pověřenec však bude vůči tomuto pracovišti plnit úlohu konzultanta a poradce.

4.5.5 Přehled činností pověřence

- Pověřenec dohlíží na všechny činnosti správce nebo zpracovatele, které se týkají ochrany osobních údajů, aniž by byla dotčena odpovědnost správce za soulad jeho postupů s Nařízením. Pověřenec zejména monitoruje, zda každé zpracování osobních údajů, které probíhá, je prováděno na základě právního titulu dle Nařízení.
- Pověřenec systematicky monitoruje dění v rámci správce nebo zpracovatele a zajišťuje udržování povědomí osob pracujících s osobními údaji o správném způsobu zpracování osobních údajů.

- Pověřenec zároveň monitoruje, zda všechny osoby, které jsou zapojeny do operací souvisejících se zpracováním osobních údajů, jsou náležitě proškolovány v oblasti ochrany osobních údajů.
- Pověřenec poskytuje informace a poradenství v oblasti ochrany osobních údajů všem osobám, které v rámci správce provádějí zpracování osobních údajů.
- Pověřenec je mentorem všech útvarů dotčených zpracováním osobních údajů, poskytuje jim na globální úrovni rady a informace, je schopen konzultovat záměry na zpracování osobních údajů a pomáhá posuzovat dopady zpracování na ochranu osobních údajů subjektů údajů.
- Pověřenec na žádost správce vypracovává posudek v souvislosti s povinností správce provádět posouzení vlivu na ochranu osobních údajů dle čl. 35 odst. 2 Nařízení.
- Pověřenec spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace s dozorovým úřadem dle čl. 36 Nařízení, a v případě vedení konzultací v jakékoliv jiné věci.
- Pověřenec je diskuzním partnerem uvnitř správce nebo zpracovatele a měl by mít zajištěn přístup do pracovních skupin správce nebo zpracovatele za účelem naplňování výše uvedených úloh.
- Pověřenec působí jako kontaktní místo pro subjekty údajů.
- Pověřenec by měl mít zajištěn přístup ke všem záznamům, které se týkají zpracování osobních údajů, zejména pokud jde o záznamy o činnostech zpracování (viz čl. 30 Nařízení), zabezpečení zpracování (viz čl. 32 Nařízení) nebo ohlašování a oznamování případů porušení zabezpečení ochrany osobních údajů (viz čl. 33 a 34 Nařízení), neboť tyto záznamy představují jeden z nástrojů umožňujících pověřenci plnit úkoly spočívající v monitorování souladu postupu správce s Nařízením a poskytování informací a poradenství správci a jednotlivým gestorům.
- Funkce pověřence spočívá mj. ve výkonu dalšího nezávislého interního auditu.
- Za předpokladu, že nedojde ke střetu zájmů, tedy pověřenci nebudou svěřeny rozhodovací kompetence v souvislosti s určováním účelů a prostředků zpracování osobních údajů, mohou být pověřenci svěřeny i další činnosti.
  Pověřenec může být zapojen například do procesu:
    - Ohlašování porušení zabezpečení osobních údajů dozorovému úřadu a oznamování porušení zabezpečení osobních údajů subjektům údajů (viz čl. 33 a 34 Nařízení). Pověřenec v rámci procesu řešení porušení zabezpečení osobních údajů může působit jako konzultant, který by se přímo nepodílel na interním vyšetřování incidentu, které bude probíhat v rámci odborných oddělení správce nebo zpracovatele, ale poskytoval by těmto výkonným článkům konzultace a rady. Rovněž pověřenec může působit jako kontaktní místo pro dozorový úřad a subjekty údajů, tedy že ohlášení či oznámení o porušení zabezpečení osobních údajů může rozesílat na příslušná místa. Zároveň je možné pověřence pověřit vedením evidence takovýchto porušení. Pověřenec by ale neměl zasahovat přímo do výkonného procesu a sám zavádět a přijímat konkrétní opatření.
    - Vedení záznamů o činnostech zpracování ve smyslu čl. 30 Nařízení. Jak stanoví výkladové stanovisko WP 29, pověřenec ve své praxi může vytvářet přehledy a vést registry operací zpracování na základě informací od jednotlivých oddělení správce nebo zpracovatele, která jsou odpovědná za zpracování osobních údajů. Článek 39 odst. 1 Nařízení nebrání správci nebo zpracovateli, aby pověřence zaúkolovali

vedením záznamů o činnostech zpracování, za něž odpovídají. Takové záznamy by měly pomoci pověřenci při plnění jeho úkolů spočívajících v monitorování souladu zpracování osobních údajů s Nařízením a rovněž při jeho poradenské činnosti[43].

- Uplatňování práv subjektů údajů dle čl. 15 – 22 Nařízení. Pověřenec by neměl být zapojen přímo do vyřizování jednotlivých žádostí, může pouze prostřednictvím poradenství a konzultací vést osoby odpovědné za výkon této agendy.

[43] Srov. Pracovní skupina podle čl. 29, Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev.01

5 Přílohy

5.1 Příloha 1 – Zpracovávané osobní údaje (Kraje)

Přehled zpracovávaných osobních údajů v krajích je uveden v dokumentu „Přehled zpracovávaných oú_KRAJE_final.xlsx“.

5.2 Příloha 2 – Zpracovávané osobní údaje (Právnické osoby zřizované kraji)

Přehled zpracovávaných osobních údajů právnických osob zřizovaných kraji je uveden v dokumentu „Přehled zpracovávaných oú_PRISPEVKOVE ORGANIZACE_final.xlsx“.

5.3 Příloha 3 – Přehled systémů (Kraje)

Dotazník přehled systémů, přehled typů systémů, rizika je uveden v dokumentu „Přehled_systémů_KRAJE_final.xlsx“.

5.4 Příloha 4 – Přehled systémů (Právnické osoby zřizované kraji)

Dotazník přehled systémů, přehled typů systémů, rizika je uveden v dokumentu „Přehled_systémů_PRISPEVKOVE ORGANIZACE_final.xlsx“.

5.5 Příloha 5 – Přehled nesouladů a doporučení (Kraje)

Přehled organizačních a technických nesouladů a doporučení je uveden v dokumentu „Přehled nesouladů_KRAJE_final.xlsx“.

5.6 Příloha 6 – Přehled nesouladů a doporučení (Právnické osoby zřizované kraji)

Přehled organizačních a technických nesouladů a doporučení je uveden v dokumentu „Přehled nesouladů_PRISPEVKOVE ORGANIZACE_final.xlsx“.

5.7 Příloha 7 – Přehled právních titulů (Kraje)

Přehled právních titulů je uveden v dokumentu „Přehled právních titulů_KRAJE_final.xlsx“.

5.8 Příloha 8 – Přehled právních titulů (Právnické osoby zřizované kraji)

Přehled právních titulů je uveden v dokumentu „Přehled právních titulů_PRISPEVKOVE ORGANIZACE_final.xlsx“.

5.9 Příloha 9 – Quick Check dotazník

Quick Check dotazník je uveden v dokumentu „Quick_Check.pdf“.

5.10 Příloha 10 – Dotazník právní

Právní dotazník je uveden v dokumentu „Dotazník_právní.xlsx“.

Tento dokument byl vypracován následující poradenskou společností:

***Grant Thornton Advisory s.r.o.**, se sídlem Jindřišská 937/16, Nové Město, 110 00 Praha 1, zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp. zn. C 86927, IČO: 265 13 960.*

Tento dokument vychází z podkladů a informací poskytnutých Klientem a je s Klientem ve fázi přípravy průběžně konzultován. Do finální akceptace Klientem je tento dokument pouze předběžným návrhem a závěry v něm obsažené jsou ve fázi přípravy a může dojít k jejich změně. Pokud chce Klient na závěry obsažené v předběžné verzi dokumentu spoléhat a činit na jejich základě jakákoli rozhodnutí, je třeba tyto závěry předem specificky potvrdit s poradenskými společnostmi. Finálně akceptovaný dokument musí být jako takový výslovně označen, jinak je považován pouze za předběžný návrh.

Zpracovatel této systémové analýzy v této souvislosti upozorňuje, že výše uvedené závěry/doporučení/mechanismy vychází ze systémové analýzy provedené na vzorku 3 krajů a 8 právnických osob zřizovaných kraji. Míru dopadu výše uvedených závěrů/doporučení/mechanismů tudíž musí posoudit každý správce osobních údajů ve smyslu čl. 4 odst. 7 GDPR, který vykonává činnosti spadající do věcné působnosti GDPR (čl. 2 odst. 1 GDPR), případ od případu a dle konkrétních okolností, zejména se zohledněním stanovených účelů, podmínek zpracování osobních údajů a úrovně zavedených organizačních a technických opatření. Odpovědný za zpracování osobních údajů v souladu s GDPR je totiž vždy správce, přičemž správce zároveň musí být schopen toto dodržení souladu doložit (čl. 5 odst. 2 a čl. 24 odst. 1 GDPR).