Ministerstvo práce a sociálních věcí
odbor sociálních služeb, sociální práce a sociálního bydlení

Doporučený postup č. 02/2018,

kterým se v rámci metodického a koncepčního vedení MPSV vypracovává Kodex chování ve smyslu čl. 40 Obecného nařízení o ochraně osobních údajů – GDPR pro potřeby výkonu sociální politiky

Určeno pro	Poskytovatele sociálních služeb, pověřené osoby, sociální pracovníky, pracovníky obecních úřadů obcí, krajské úřady a dotčené útvary MPSV
Datum platnosti:	9. dubna 2018
Datum účinnosti:	25. května 2018
Vypracoval:	Odbor 22
Verze:	1.3
Počet stran:	30

Obsah

Historie verzí a změn

Číslo verze	Datum verze	Popis	Seznam změn
1.0	5. 4. 2018	Úvodní verze dokumentu	
1.1	9. 4. 2018	Zapracování informačního stanoviska ÚOOÚ	1. Doplnění historie verzí a změn 2. Změna doporučení na **nepoužívat** DPO u příspěvkových organizací (kap. 2.2) 3. Drobné korektury textu
1.2	9. 5. 2018	Zapracování změn výkladové praxe a korektur dokumentu	1. V kap. 1.2 upravena definice rozsahu platnosti nařízení s ohledem na aktuální interperetaci nálezu US 38/02 z 9. 3. 2004 2. V kap. 3.1 doplněna věta k možnosti odmítnutí souhlasu se zpracováním OÚ, pokud je možnost služby poskytovat anonymně. 3. V kap. 3.1 upřesněna aplikace hranice 15 let v souvislosti se službami informační společnosti. 4. Zdůrazněno omezení používání Přílohy č. 4 pro výjimečné případy v kap. 4.7. 5. Upřesnění formulace volby pověřence v kap. 4.10. 6. Změna zvýrazněné formulace v závěru kap. 4.6. 7. Odložení publikace chybějících příloh ke dni 23. 5. Z důvodu jejich dosud neujasněné podoby. 8. Aktualizovaná znění příloh č. 1., 3., 7. a 8. 9. Drobné korektury textu.

1.3	4. 6. 2018	Zapracování postupu hlášení bezpečnostních incidentů, doplnění povinnosti jmenovat DPO pro DOZP a formalizace posouzení vlivu.	1. Upřesnění výjimek, kdy je nezbytné jmenovat DPO (kap. 2.2) 2. Upřesnění vyhodnocování, evidence a hlášení bezpečnostních incidentů (kap. 4.8) 3. Upřesnění povinnosti a provedení posouzení vlivu (DPIA – viz. kap. 4.9)

1. ÚVOD

1.1. Účel kodexu chování

Tento kodex si klade za cíl ulehčit implementaci a aplikaci nařízení GDPR, tj. obecného nařízení Evropské unie o ochraně osobních údajů č. 2016/679, subjektům působícím v oblasti výkonu sociální politiky v prostředí České republiky. Jeho účelem není nahradit právní úpravu nařízení GDPR ani doporučené postupy či výkladová stanoviska Úřadu pro ochranu osobních údajů („ÚOOÚ“) či celoevropské pracovní skupiny WP29, ale má sloužit jako jejich doplněk a obecné interpretační vodítko při aplikaci jednotlivých zásad ochrany osobních údajů a jednotlivých povinností upravených nařízením GDPR v prostředí sociálních služeb ve smyslu čl. 40 GDPR. Tento materiál se věnuje výkladu právní úpravy ochrany osobních údajů způsobem, který interpretuje relevantní články nařízení GDPR jako konkrétní praktická opatření k dosažení souladu s nařízením GDPR, a který by tak měl zjednodušit jeho zavedení do praxe. Uvedenému záměru odpovídá i struktura níže předloženého materiálu, kdy po obecném úvodu a vysvětlení, v čem spočívají zásadní změny nové právní úpravy, se další kapitoly věnují výkladu jednotlivých zásad zpracování osobních údajů a jednotlivých povinností správců a zpracovatelů a jejich praktickému uchopení.

Tento kodex je určen pro výkon sociální politiky, tj. všem poskytovatelům sociálních služeb, pověřeným osobám SPOD, sociálním pracovníkům, a pracovníkům obcí, krajských úřadů a MPSV, kteří vykonávají sociální agendy a nějakým způsobem zpracovávají osobní údaje (také jako „OÚ“), tj. jakékoliv informace o konkrétní identifikované fyzické osobě (např. zdravotnická dokumentace se jménem klienta či spis konkrétního zaměstnance) či jakékoliv informace umožňující tuto identifikaci (např. jméno a příjmení, fotografie). Každý poskytovatel sociálních služeb, sociální pracovník, nebo většina pověřených osob (s výjimkou pěstounů) v nějaké fázi své existence či činnosti osobní údaje zpracovává, a pokud nikoliv u klientů (např. anonymně poskytované služby bez pořizování záznamů[1]), tak alespoň u svých zaměstnanců, zástupců klientů, kontaktních a spolupracujících osob apod..

Předložený materiál je zpracován obecně pro všechny formy výkonu sociální politiky a jedná se o dobrovolný a doporučený podklad zpracovaný MPSV v rámci povinnosti metodického vedení externích subjektů provádějících výkon sociální politiky, tj. v roli subjektu zastupujícího výše uvedené kategorie správců a zpracovatelů osobních údajů v oblasti sociální politiky ve smyslu čl. 40 odst. 2 GDPR. Materiál bude po přijetí a nabytí účinnosti adaptačního zákona a ustavení dozorového úřadu (kterým se předpokládá ÚOOÚ) předložen ke schválení, registraci a zveřejnění ve smyslu čl. 40 odst. 5 a 6 GDPR. Podle aktuálních vyjádření ÚOOÚ se však nepředpokládá vydání jeho schválení před koncem prvního pololetí 2019.

Přílohou kodexu chování jsou vzory a formuláře pro implementaci povinností vyplývajících z nařízení GDPR, které budou (stejně jako vlastní text kodexu) průběžně doplňovány v souladu s budoucí výkladovou praxí a stanovisky dozorového úřadu.

1 **Plně anonymizované údaje**, u nichž nelze dohledat, k jaké konkrétní fyzické osobě se vztahují, **nejsou osobními údaji**; pseudonymizované osobní údaje se již za osobní údaje považují.

1.2. Nařízení GDPR obecně

Nařízení GDPR je zkrácený název z anglického označení **nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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)**, (v textu jako „GDPR" nebo „nařízení GDPR"). Toto nařízení se dnem nabytí účinnosti 25. května 2018 stává přímo aplikovatelným právním předpisem na území všech členských států Evropské unie (s použitím i pro zbývající členské země EHP), kdy na území České republiky fakticky nahrazuje stávající zákon č. 101/2000 Sb., o ochraně osobních údajů. Oficiálně zrušit tento zákon a upravit některé otázky ponechané v působnosti členských států EU má nový zákon České republiky doprovodný k nařízení GDPR, s jehož přijetím se počítá v průběhu roku 2018 (dále také jako „zákon o zpracování osobních údajů", nebo „adaptační zákon").

Právní úprava GDPR ve své podstatě **nepředstavuje revoluci v oblasti ochrany osobních údajů**, ale je jenom přirozeným posunem v dosavadním právním vývoji, který reaguje na faktické změny, zejména na technologický vývoj a s ním spojené nové hrozby. Subjekty, které dosud věnovaly pozornost otázce ochrany osobních údajů a plnění svých povinností, tedy nemusí mít obavy z implementace nařízení GDPR. Je ovšem potřeba zohlednit, že správcům a zpracovatelům přibylo několik nových povinností a že nová právní úprava přináší i některé další změny. Mezi nejvýznamnější novinky patří:

1. přesunutí povinnosti prokázat soulad s nařízením GDPR na správce – nově již dozorové úřady při kontrole nemusí aktivně zjišťovat konkrétní porušení povinností dotčeného subjektu, ale tento dotčený subjekt musí sám předložit důkazy, kterými prokáže správnost svých postupů;
2. nový institut osvědčení o souladu s nařízením GDPR – jeden ze způsobů, jak prokázat soulad s nařízením GDPR ve smyslu předchozího bodu; osvědčení budou vydávat akreditované subjekty s platností na dobu max. 3 let;
3. opuštění souhlasu subjektu údajů se zpracováním OÚ jako základního právního titulu a zpřísnění podmínek k získání souhlasu – tam, kde lze zpracování OÚ založit na jiném právním titulu (např. plnění smlouvy uzavřené se subjektem údajů, plnění zákonné povinnosti, realizace oprávněných zájmů správce), má přednost tento titul a získání souhlasu subjektu údajů je nežádoucí;
4. nový právní titul ke zpracování OÚ – zpracování OÚ je zákonné též tehdy, je-li nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
5. opuštění oznamovací povinnosti (notifikace zpracování OÚ) vůči ÚOOÚ – v zásadě ji nahrazuje nová povinnost vést záznamy o činnostech zpracování ve smyslu čl. 30 GDPR, která dopadá na stanovený okruh správců a zpracovatelů;
6. zavedení povinnosti jmenovat pověřence pro ochranu osobních údajů – dopadá na vymezené skupiny správců a zpracovatelů; blíže viz čl. 37 a násl. GDPR;
7. nová povinnost ohlašování a oznamování bezpečnostních incidentů a nová povinnost provedení posouzení vlivu a předchozí konzultace s dozorovým úřadem;
8. vyšší limit maximálních pokut (až 10 mil. Kč, dle předběžného stanoviska ÚOOÚ).

Úprava nařízení GDPR chrání **pouze osobní údaje žijících fyzických osob** (osobními údaji ve světle tohoto právního předpisu jsou pouze údaje vztahující se k fyzickým osobám) a nevztahuje se na údaje právnických osob, nebo údaje fyzických osob spojené s výkonem jejich funkce, nebo zaměstnání, pokud jsou tyto údaje zveřejňovány v oprávněném zájmu správce, tj. pro výkon jeho činnosti a garance její kvality. Nařízení GDPR se také nevztahuje na osobní údaje zesnulých osob, je ovšem nutné si uvědomit, že ochranu vyžadují takové osobní údaje o zesnulých, které by mohly vypovídat také něco o žijících osobách (např. údaje o dědičné nemoci), nebo údaje které jsou chráněny jinými právními předpisy (např. zdravotnická dokumentace).

2. VÝKON SOCIÁLNÍ POLITIKY

2.1. Okruhy zpracovávaných údajů

Výkon sociální politiky konkrétními subjekty je prováděn pomocí služeb v pobytové, ambulantní nebo terénní formě. Při své činnosti tyto subjekty osobní údaje zpravidla shromažďují a ukládají do listinných (fyzických) kartoték či do elektronických složek a databází. Nařízení GDPR se přitom vztahuje právě (i) na manuální zpracování (tedy s přítomností lidského prvku) osobních údajů, které jsou nebo mají být zařazeny do evidence, tj. do záznamů umožňujících vyhledávání dle určitých hledisek, a/nebo (ii) na zcela nebo částečně automatizované zpracování osobních údajů. Ve smyslu nařízení GDPR je tedy zpracováním osobních údajů i používání emailového klienta umožňujícího vyhledávání v příchozí a odchozí poště.

Z praxe lze shrnout, že zpravidla jsou zpracovávány osobní údaje:

1. ohledně následujících okruhů subjektů údajů (pouze FO): klienti, jejich rodinní příslušníci, zájemci o sociální služby, zaměstnanci, dobrovolníci, uchazeči o zaměstnání, dodavatelé nebo jejich zástupci (např. statutární orgán), sponzoři, dárcové atd.;
2. zejména v rozsahu: identifikační údaje (jméno, příjmení, rodné číslo, datum narození), kontaktní údaje (adresa, telefonní číslo, email), klientské údaje (o poskytovaných službách, zdravotním stavu, rasovém či etnickém původu, atd.), zaměstnanecké údaje (o průběhu pracovního poměru, údaje související s mzdovou agendou, daňovou agendou a agendou sociálního a zdravotního pojištění, např. výše mzdy či číslo bankovního účtu), údaje o sponzorech a dárcích (výše různých příspěvků a darů, čísla bankovních účtů), fotografie a audiovizuální záznamy z pořádaných akcí (zobrazující konkrétní osoby), záznamy získané vstupními a docházkovými systémy;[2]
3. zejména za účelem: výkonu sociální politiky (tj. zejména poskytování sociálních služeb, výkonu sociální práce a plnění povinnosti pověřené osoby)[3], plnění povinností příjemce dotace, vedení účetnictví, zpracování personální agendy, propagace své činnosti;

2 Je-li prováděn monitoring zaměstnanců (GPS tracking vozidel, záznamy tel. hovorů, kontrola emailů), je nezbytné kromě nařízení GDPR dostát i právní úpravě zákoníku práce (§ 316 ZP) a související judikatuře.

3 Především v rozsahu zák. č. 108/2006 Sb., o sociálních službách, ve znění pozdějších předpisů a zák. č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů.

4. s rizikem úniku či zneužití ze strany: zaměstnanců s přístupem k osobním údajům (včetně agentových pracovníků, brigádníků a pracovníků na dohodu o provedení práce, nebo pracovní činnosti), zpracovatelů (mzdová účtárna, účetní, správa budov apod.), externích osob s přístupem k OÚ (poskytovatelé IT služeb, daňoví poradci, dodavatelé), ale i jiných správců údajů, jako jsou veřejné správní a kontrolní orgány, poskytovatelé podpor, organizátoři exkurzí, sponzorských akcí apod.[4]

Z výše uvedeného je zřejmé, že v rámci výkonu sociální politiky jsou často zpracovávány citlivé údaje (slovy GDPR „zvláštní kategorie osobních údajů", jejichž uzavřený výčet je upraven v čl. 9 odst. 1 GDPR), jako jsou např. údaje o zdravotním stavu, o rasovém či etnickém původu, náboženském vyznání, či sexuální orientaci, které vyžadují vyšší míru ochrany.

2.2. Pověřenec pro ochranu osobních údajů

Jedním z nejdiskutovanějších témat u správců a zpracovatelů je otázka, na které subjekty vlastně dopadá povinnost jmenovat pověřence pro ochranu osobních údajů1 (dále také jako „pověřenec"), nicméně ihned v úvodu je nezbytné zdůraznit, že **dobrovolnou možnost jmenovat pověřence má každý správce a zpracovatel.**

Dle čl. 37 odst. 1 nařízení GDPR má povinnost jmenovat pověřence:

a) orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;

b) správce či zpracovatel, jehož hlavní činnosti spočívající ve zpracování OÚ vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo

c) správce či zpracovatel, jehož hlavní činnosti spočívají v rozsáhlém zpracování citlivých údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.

Všechny subjekty, které jsou zároveň orgánem veřejné moci či veřejným subjektem, jsou tedy dle výše uvedeného článku povinny ustanovit pověřence bez dalšího. Důvodem pro toto pravidlo by měla být potřeba zvýšené kontroly u subjektů, které vykonávají veřejnou moc a které tedy mohou i autoritativně (jednostranně) rozhodovat o právech a povinnostech druhé strany (subjektu údajů); v těchto nikoli rovnoprávných vztazích mají totiž subjekty údajů velmi malou možnost ovlivnit, zda a jak budou jejich osobní údaje zpracovány. Do kategorie orgánů veřejné moci a veřejných subjektů spadají nepochybně organizační složky státu, včetně ministerstev ČR, územní samosprávné celky (obce, kraje) a jejich organizační složky.

V rámci tohoto kodexu chování se ustavuje, že **veřejnými subjekty ve smyslu čl. 37 GDPR nejsou příspěvkové organizace** zřízené organizačními složkami státu dle zákona č. 218/2000 Sb., o rozpočtových pravidlech, či územními samosprávnými celky dle zákona č. 250/2000 Sb.,

4 Každý správce nese odpovědnost za zákonnost svého postupu sám.

o rozpočtových pravidlech územních rozpočtů[5]. V obecném chápání i podle logiky předpisů o přístupu k informacím totiž příspěvkové organizace za veřejné subjekty považovány jsou. Podléhají správním řízením, kontrolám i rozpočtovým opatřením a jsou příjemci dotačních titulů. **Ve smyslu čl. 37 odst. 4 GDPR tak pro příspěvkové organizace zřízené organizačními složkami státu, či územními samosprávnými celky při přihlášení se k tomuto kodexu neplatí povinnost jmenovat pověřence.**

Důsledkem pověření ke zřizování zařízení pro děti vyžadující okamžitou pomoc je založení působnosti pověřené osoby k výkonu veřejné správy, a to při rozhodování ředitele zařízení pro děti vyžadující okamžitou pomoc o některých právech a povinnostech účastníků souvisejících s pobytem dítěte v zařízení (§ 42a odst. 4, § 42b odst. 3 ZSPOD), kdy ředitel zařízení rozhoduje v postavení správního orgánu, tedy v rámci správního řízení. **Pro zařízení pro děti vyžadující okamžitou pomoc (ZDVOP) tedy platí povinnost mít ustanoveného pověřence pro ochranu osobních údajů.**

Obdobně lze vzhledem k možnosti správního rozhodování o nepovolení pobytu dítěte mimo zařízení ředitele domovů pro osoby zdravotně postižené (DOZP) aplikovat povinnost mít pověřence, tj. **pro domovy pro osoby zdravotně postižené (DOZP) platí povinnost mít ustanoveného pověřence pro ochranu osobních údajů, pokud pracují s dětskými klienty.**

Při výkonu sociální politiky se téměř nikdy nejedná o případ, kdy by zpracování osobních údajů bylo hlavní činností subjektu. Přestože lze konstatovat, že je prováděno monitorování subjektů údajů či zpracování jejich osobních údajů a tato činnost je pravidelná i systematická, je nutné zohlednit, že se jedná pouze o podpůrné činnosti k vlastnímu výkonu sociální politiky. Z existence mnoha služeb vykonávaných anonymně lze také částečně dovodit oddělitelnost výkonu sociální politiky od zpracování osobních údajů. Na rozdíl od nemocnice (výslovně zmíněné ve stanovisku WP29), kde není možné oddělit zpracování údajů od poskytování péče, aby nedošlo k zdravotním komplikacím, se v případě sociálních služeb jedná jen velmi výjimečně o přímou vazbu služby a konkrétního klienta (tím samozřejmě není rozporován přínos takovýchto vazeb ke kvalitě služeb a zvýšení uživatelského komfortu klienta). Zároveň lze zpochybnit i otázku rozsáhlého zpracování údajů, které jsou v rámci výkonu sociální politiky monitorovány, nebo zpracovávány. Dle pracovní skupiny WP29 pro posouzení otázky rozsáhlosti zpracování osobních údajů nutno vzít v úvahu: (i) počet dotčených subjektů údajů; (ii) objem zpracovávaných osobních údajů a/nebo jejich škálu; (iii) trvání nebo stálost zpracování; a (iv) zeměpisný rozsah zpracování.

Realita výkonu sociální politiky je různorodá, ale lze zjednodušeně říci, že:

1. pobytové služby jsou vzhledem k omezené kapacitě současně poskytovány v průměru desítkám klientů;
2. ambulantní nebo terénní služby jako mírně kapacitnější jsou poskytovány řádově stovkám klientů a
3. subjekty se zaměstnanci a externími spolupracovníky pro ně zpracovávají údaje výlučně z titulu plnění svých povinností coby zaměstnavatelů v rámci běžné zaměstnanecké agendy (např. mzdová agenda či agenda sociálního a zdravotního pojištění), nebo vzhledem k výkonu jejich činnosti (např. údaje o zdravotním stavu, o velikostech pracovního oblečení a ochranných pomůcek apod.).

5 Uvedené vychází z předběžného stanoviska ÚOOÚ ze dne 29. 3. 2018.

Poskytovatelé tedy nezpracovávají značné množství osobních údajů na celostátní ani regionální úrovni, jako je tomu například u krajských nemocnic, ale jejich situace se spíše blíží zpracování osobních údajů jednotlivými lékaři nebo zdravotníky. Přitom situace jednotlivých lékařů dle nařízení GDPR (viz. recitál č. 91) by neměla být považována za situaci zpracování osobních údajů ve velkém rozsahu.

Obecně tedy platí, že s výjimkou uvedenou výše pro zařízení pro ZDVOP a vybrané DOZP **subjekty vykonávající sociální politiku, které nejsou veřejnými subjekty, povinnost jmenovat pověřence nemají** (mohou tak samozřejmě učinit dobrovolně, např. z důvodu své celostátní působnosti a snahy o minimalizaci rizik spojených se zajištěním souladu s GDPR).

3. ZÁKLADNÍ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Základní zásady jsou důležitým interpretačním a aplikačním vodítkem, nejen v případě sporných otázek; také se v nich odrážejí jednotlivé povinnosti. Je tedy důležité si uvědomit, že dodržení určité konkrétní povinnosti podle GDPR bude vykládáno též prostřednictvím dodržení základních zásad. Zásady tedy nejsou jenom bezobsažně teoretické, ale významně napovídají, jak v praxi postupovat. Zásady jsou formulovány zejména v čl. 5 nařízení GDPR.

3.1. Zákonnost

Zásada zákonnosti představuje obecnou povinnost postupovat v souladu s pravidly GDPR, ale i specifickou povinnost **mít konkrétní činnost zpracování OÚ založenou na jednom z právních titulů** (viz. výčet titulů v čl. 6 odst. 1 GDPR, a jedná-li se o zvláštní kategorie osobních údajů, tj. citlivé údaje, viz čl. 9 odst. 2 GDPR); zpravidla se realizuje například:

1. shromažďování a uložení OÚ klienta z titulu plnění smlouvy o výkonu služeb nebo jedná-li se o zpracování citlivých údajů, z titulu poskytování sociální nebo zdravotní péče;
2. zpracování mzdových údajů zaměstnanců z titulu plnění zákonných povinností;
3. zpracování osobních údajů kontaktních osob, opatrovníků klientů či jiných třetích osob nežli klientů z titulu plnění zákonné povinnosti řádného poskytování sociální služby;
4. provozování kamerového systému z titulu oprávněných zájmů správce, jako je ochrana majetku či osob v prostorách poskytovatele.

Právní tituly se v časovém horizontu vyvíjejí – osobní údaje uchazeče o zaměstnání se zpracovávají, nebo i krátkodobé (v horizontu roku) ukládání kontaktních údajů na neúspěšné uchazeče z titulu uzavření budoucí smlouvy v oprávněném zájmu, stane-li se zaměstnancem, z velké většiny z titulu plnění zákonných povinností, je-li veden spor o platnost výpovědi z titulu opět oprávněných zájmů poskytovatele – je proto vhodné přemýšlet nad zpracováním osobních údajů jako o dynamickém

procesu. Není vyloučeno ani to, aby v jednom momentu pro jeden úkon zpracování existovalo více právních titulů.

Jak již bylo naznačeno, každý správce nebo zpracovatel by si měl detailně **zmapovat, jakými tituly jsou kryty jednotlivé úkony či činnosti zpracování OÚ**, tedy posoudit si, proč a za jakým účelem zpracovává ty které osobní údaje a který zákonný titul mu pro to svědčí (viz. Příloha č. 1 – Vzor katalogu osobních údajů). Tam, kde lze osobní údaje zpracovávat i z jiného právního titulu, než je souhlas subjektu údajů s tímto zpracováním, nedoporučuje se žádat/získávat souhlas subjektu údajů, jelikož je to: (i) pro subjekt údajů matoucí, tj. klient či zaměstnanec se může domnívat, že pokud souhlas odvolá, jeho osobní údaje dále nebudou zpracovávány); a (ii) pro správce zbytečně zatěžující z hlediska administrativy. **Specificky u zaměstnanců by se souhlas měl získávat pouze výjimečně, protože se dovozuje, že zaměstnanec z povahy věci nemůže poskytnout souhlas svobodně.**

Také je vhodné, aby klient služby byl kvalifikovaně informován o zpracování jeho osobních údajů a měl možnost, pokud to služba umožňuje, výslovně požadovat anonymní poskytnutí služby.

Je-li souhlas subjektu údajů se zpracováním OÚ nezbytný (může tomu tak být např. za účelem pořízení a zveřejnění fotografií z různých akcí zobrazujících klienty), je potřeba pamatovat na požadavky nařízení GDPR, kdy **souhlas má být**:

1. **svobodný a aktivní** – nesmí být předpokládán např. před-zaškrtnutým políčkem v elektronickém dokumentu; správce by neměl vyžadovat udělení souhlasu ke zpracování osobních údajů jako podmínku poskytování sociální služby (zákaz „take it or leave it“) – zpracování OÚ nezbytné pro výkon sociální politiky bude zpravidla kryto titulem plnění smlouvy nebo zákonné povinnosti či titulem oprávněného zájmu při poskytování sociální nebo zdravotní péče;
2. **konkrétní a jednoznačný** – pro jednotlivé účely či úkony zpracování musí být souhlas udělen jednotlivě;
3. **informovaný** – srozumitelná formulace souhlasu s uvedením vyžadovaných údajů o zpracování a s náležitým poučením o právech subjektu údajů (právo na opravu/doplnění údajů, právo na odvolání souhlasu, apod.);
4. **„viditelný“ a „odlišitelný“** – pokud souhlas není udělován na samostatném dokumentu, měl by být dostatečně graficky oddělený, a tak odlišitelný od zbytku textu (u smluv se doporučuje, aby textace souhlasu následovala až po podpisu smlouvy, nejlépe však, aby byla na samostatném dokumentu);
5. **snadno odvolatelný** – odvolání souhlasu by mělo být stejně snadné, jako jeho udělení (např. zpřístupnění jednoduchého webového formuláře);
6. **oddělitelný** – nesmí být spojován s jinými požadavky

V případě zpracování osobních údajů **dětí** ze strany správce, které vyžaduje souhlas se zpracováním osobních údajů, je pro určení osoby, která by souhlas měla udělit, rozhodující zejména úprava občanského zákoníku. **Nařízení GDPR se totiž věnuje výslovně pouze souhlasu dítěte v souvislosti se službami informační společnosti**, kdy dítě ve věku 16 let a více je vždy považováno za způsobilé

udělit souhlas samo.[6] Občanskoprávní úprava pracuje s konceptem postupného nabývání způsobilosti k právnímu jednání, přičemž lze konstatovat, že dítě nejpozději v 15ti letech již souhlas se zpracováním osobních údajů uděluje samo a souhlas zákonného zástupce se nepožaduje.

3.2. Korektnost a transparentnost

Zásada je vyjádřením požadavku, aby jakékoliv informace určené subjektům údajů či veřejnosti, byly na jednu stranu pregnantní, úplné a správné, a na druhou stranu stručné, srozumitelné, podávané za použití „jasných a jednoduchých jazykových prostředků“. Ve vhodných případech lze zvolit i vizualizaci např. prostřednictvím piktogramů. V této souvislosti **je vhodné, aby správci a zpracovatelé zrevidovali a aktualizovali všechny své informační materiály a dokumenty obsahující relevantní informace**, jako jsou poučení doprovázející souhlas se zpracováním OÚ či zveřejněné zásady ochrany osobních údajů, aby tyto byly jazykově přístupnější a obsahovaly aktuální informace o právech subjektů údajů.

3.3. Účelové omezení

Osobní údaje mají být **zásadně používané za účelem, pro který byly původně získané** (shromážděné), a neměly by být zpracovávány způsobem, který je s tímto účelem neslučitelný (např. identifikační a kontaktní údaje dárců shromážděné za účelem správy darů a vystavení potvrzení pro daňové účely by nepochybně neměly být zpřístupněné komerčním subjektům pro nabídku jejich zboží a služeb). Pokud by mělo dojít ke zpracování osobních údajů pro jiný než původní účel, správce by měl slučitelnost účelů posoudit s ohledem na vazbu mezi původním a zamýšleným účelem, okolnosti shromáždění OÚ, povahu osobních údajů (zejména zda se nejedná o citlivé údaje), možné důsledky dalšího zpracování pro subjekty údajů a existenci vhodných záruk ochrany osobních údajů. Slučování účelů zpracování bez souhlasů subjektů údajů se nedoporučuje. Za neslučitelné se nepovažuje další zpracování pro účely archivace ve veřejném zájmu (např. archivace mzdových listů, daňových dokladů či zdravotnické dokumentace po zákonem stanovenou dobu), pro účely vědeckého či historického výzkumu nebo pro statistické účely.
Jako u právních titulů zpracování platí, že i účely zpracování se mohou v čase vyvíjet.

3.4. Minimalizace údajů

Osobní údaje klientů, zaměstnanců a dalších subjektů údajů, které jsou při výkonu sociální politiky získávané a jsou dále zpracovávané, by měly být přiměřené, relevantní a **omezené na nezbytný rozsah ve vztahu k účelu**, pro který jsou zpracovávány. Správci by si měli posoudit, zda opravdu potřebují všechny údaje, které mají shromážděné a uložené, a toto posouzení by měli pravidelně provést ve vztahu ke všem zpracovávaným údajům, resp. se doporučuje vytvořit si postupy, jak efektivně minimalizovat objem a rozsah zpracovávaných dat (např. při obdržení dokumentu

6 Návrh nového zákona o zpracování osobních údajů snižuje tuto stanovenou hranici na 13 let.

automaticky začernit nepotřebné údaje). U zaměstnanců zcela jistě není potřeba zpracovávat údaje o jejich národnosti či zálibách; životopisy uchazečů u zaměstnání nejsou aktuální déle než jeden či dva roky atd. Je potřeba pamatovat na to, že účely zpracování se v čase mění, a tomu je potřeba přizpůsobit i objem a rozsah zpracovávaných údajů – např. spis zaměstnance zpravidla by neměl být po ukončení pracovního poměru uchováván v původním rozsahu.

3.5. Přesnost

Všichni správci a zpracovatelé jsou povinni zpracovávat přesné a v případě potřeby aktualizované osobní údaje. Musí být zároveň přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny – je potřeba zavést mechanizmy pravidelné kontroly přesnosti a správnosti zpracovávaných osobních údajů. Pokud je to možné, musí být o změně informován subjekt, kterého se změna týká (dotčenou osobu), např. použitím Přílohy č. 6 - Vzor – Oznamovací povinnost o změně osobních údajů.

Musí být zachován důkaz, na základě, kterého byla změna zrealizována, resp. výmaz. V opačném případě by mohlo dojít k zásahu do práv subjektů údajů, např. neaktualizované údaje o osobním stavu zaměstnance a počtu jeho dětí by mělo za následek určení nesprávné výše daně z příjmů. Zároveň je potřeba pamatovat na tzv. „historická“ data, kdy je důležité uchovávat vedle aktuálních osobních údajů i osobní údaje původní, jako je to v případě zdravotnické dokumentace.

3.6. Omezení uložení

V souladu s obecným důrazem na minimalizaci zpracování osobních údajů nařízení GDPR vyžaduje, aby **osobní údaje nebyly uchovávány (zpracovávány) po dobu delší, než je nezbytné s ohledem na účely zpracování**; např. kontaktní údaje uchazečů o zaměstnání, kteří nebyli přijati, mají relevanci pouze omezenou dobu. Osobní údaje lze uchovávat déle, než je nezbytné pro původní účel, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření pro zaručení práv a svobod subjektů údajů. Takovým opatřením může být např. pseudonymizace zdravotnické dokumentace zesnulých klientů, která je uchovávána za účelem povinné archivace.[7]

7 Doby uchování zdravotnické dokumentace upravuje vyhláška č. 98/2012 Sb. Pro archivování jiných dokumentů týkajících se klienta, jejichž doba uchování není upravena právním předpisem, platí dle standardů kvality poskytování sociálních služeb, že poskytovatel má stanovit dobu pro uchování dokumentace o osobě po ukončení poskytování sociální služby.

3.7. Integrita a důvěrnost

Nařízení GDPR klade důraz na náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických a organizačních opatření **před neoprávněným či protiprávním zpracováním (únikem) a před náhodnou ztrátou, zničením nebo poškozením**. Opatření je nutné volit dle konkrétní situace poskytovatele sociálních služeb – listinná (fyzická) kartotéka bude chráněna fyzickým uzamčením, vhodným umístěním v rámci objektu či umožněním přístupu pouze odpovědným osobám; elektronická evidence bude zabezpečena přístupovými hesly a náležitou ochranou koncových zařízení (antivirová ochrana počítačů, tabletů či chytrých telefonů). Pro ochranu před ztrátou údajů jsou důležité bezpečnostní zálohy údajů. I když je nařízení GDPR založeno na principu technologické neutrality, doporučuje možná technická opatření k ochraně OÚ, jako je pseudonymizace nebo šifrování. Pseudonymizací ve smyslu GDPR se chápe reverzibilní postup, kdy identifikační údaje (jméno a příjmení, datum narození atd.) jsou odděleny od zbytku uchovávaných osobních údajů a jsou nahrazeny unikátním bezvýznamovým identifikátorem. Šifrováním ve smyslu GDPR se chápe reverzibilní postup převodu hodnot jednotlivých údajů prostřednictvím klíče (šifry) na bezvýznamový řetězec znaků. Úroveň šifrování, případně hodnocení náročnosti prolomení šifry není v rámci nařízení GDPR stanoveno, ale mělo by odpovídat technickým a personálním možnostem konkrétního správce nebo zpracovatele.

Každý správce nebo zpracovatel by si tedy měl zmapovat svůj systém zpracování osobních údajů celkově i jeho jednotlivé prvky, tj. procesy jak jsou osobní údaje získávány, kde jsou uloženy, kdo k nim má přístup (viz. Příloha č. 1: – Vzor – Katalog osobních údajů a Příloha č. 3: Vzor – Záznam o činnostech zpracování), identifikovat a analyzovat rizika s těmito údaji spojená (viz. Příloha č. 2: – Vzor – Analýza rizik) a navrhnout a zavést, resp. aktualizovat, systém vhodných a odpovídajících opatření ochrany osobních údajů (de facto se jedná o nápravná opatření spojená s identifikovanými riziky a průběžné vyhodnocování jejich účinnosti, případně jejich revize).

3.8. Odpovědnost správce

Každý správce nese odpovědnost za dodržení výše uvedených základních zásad, ale i **za celkový soulad zpracování osobních údajů s nařízením GDPR** (viz. čl. 24 GDPR). Každý správce musí být zároveň schopen doložit tento soulad; o možných způsobech prokázání souladu je blíže pojednáno v kapitole 4.1.

4. DESATERO POVINNOSTÍ A ODPOVÍDAJÍCÍ OPATŘENÍ

Pro účely kodexu byly jednotlivé povinnosti správců a zpracovatelů dle GDPR rámcově shrnuty do desatera povinností. Následující kapitoly se tedy detailněji věnují těmto deseti základním okruhům povinností, a dále odpovídajícímu způsobu, jak těmto povinnostem dostát.

4.1. Prokázat soulad s nařízením GDPR

Zásadní a ostatní povinnosti zastřešující je povinnost všech správců údajů prokázat soulad s úpravou nařízení GDPR, tedy vlastně prokázat naplňování ostatních povinností. Kromě přihlášení se k tomuto kodexu se jedná především o zdokumentování situace v oblasti osobních údajů, kdy:

1. dokumentace by měla obsahovat informace o situaci zpracování osobních údajů, tj. jaké údaje, za jakým účelem a jak a kým se zpracovávají atd. (viz. Příloha č. 1: Vzor – Katalog osobních údajů) a o systému přijatých opatření (viz. Příloha č. 2: Vzor – Katalog rizik);
2. součástí dokumentace mají být dále: záznamy o činnostech zpracování (čl. 30 GDPR – viz. Příloha č. 3: Vzor – Záznam o činnostech zpracování); zásady správce v oblasti ochrany osobních údajů (např. ve formě kodexu chování); vnitřní směrnice o pravidlech zpracování OÚ (interní dokument, kterým se zejména správce přihlašuje ke kodexu chování a zavazuje svoje zaměstnance a spolupracující subjekty dodržováním nařízení GDPR), přijatých opatřeních a zavedených postupech (viz. Příloha č. 2: Vzor Katalog rizik); záznamy o provedených školeních zaměstnanců; vzory souhlasů subjektů údajů (souhlasy musí být aplikovány na obsah a účel podle jednotlivých konkrétních položek katalogu osobních údajů); příslušné smlouvy se zpracovateli a příjemci osobních údajů (vzory příslušných ustanovení zveřejní dozorový úřad)[8].

4.2. Dodržovat zásady zpracování osobních údajů

Zásady GDPR se do značné míry neliší od zásad, na nichž je postavena právní úprava před přijetím GDPR. Novinkou je zejména zesílená zásada odpovědnosti správce a z ní vyplývající povinnost správce být schopen prokázat soulad s GDPR. Jednotlivé zásady zpracování osobních údajů jsou blíže rozvedeny v předchozí kapitole 3.

8 Dle § 52 odst. 1) písm. g) adaptačního zákona – návrh znění k 1. 4. 2018

4.3. Používat vhodná technická a organizační opatření

Nařízení GDPR stanoví pro všechny správce povinnost **zavést a pravidelně aktualizovat** systém tzv. technických a organizačních opatření („TOMs“; *z angl. Technical and Organisational Measures*). **Každý správce by měl nejenom zavést vhodná a přiměřená opatření, ale také v průběhu své činnosti v rozumných časových intervalech sledovat a vyhodnocovat situaci osobních údajů a reagovat na případné změny** (např. přechod na cloudové úložiště, digitalizace dříve listinných kartoték, umožnění zaměstnancům pracovat z domova apod.) aktualizací těchto opatření.

GDPR poskytuje vodítko pro implementaci TOMs v tom smyslu, že **jejich implementace by měla zohlednit**: (i) charakter zpracování OÚ; (ii) rizika zpracování OÚ; (iii) stav techniky; a (iv) náklady na provedení. Toto vodítko je odrazem zásady přiměřenosti, která se prolíná celým GDPR. Znamená, že je nutno vzájemně zohlednit na straně jedné zejména rizika zpracování pro subjekty údajů vyplývající z rámce (povahy, rozsahu) zpracování OÚ při výkonu sociální politiky, a na straně druhé zejména faktické možnosti na straně správce nebo zpracovatele, a to zejména pokud jde o stav techniky, tak z hlediska nákladů na provedení.

Mezi technická a organizační opatření, která lze dle konkrétní situace aplikovat, patří například:

1. opatření **fyzické ochrany**, jako je ostraha a zabezpečení objektu a místností, mříže, fyzické umístění serverů a koncových zařízení;
2. opatření **ochrany na úrovni IT**, jako je antivirová a antispamová ochrana, správa účtů a hesel, omezení přístupu do zaměstnaneckých mobilních zařízení;
3. bezpečnostní zálohy;
4. bezpečnostní směrnice;
5. školení zaměstnanců v oblasti ochrany osobních údajů a manuál / vnitřní směrnice s pravidly a postupy pro snadnější orientaci zaměstnanců;
6. dokumentace TOMs i další dokumentace pro oblast ochrany osobních údajů.

4.4. Minimalizovat zpracování osobních údajů

Povinnost minimalizovat zpracování osobních údajů je odrazem principu minimalizace údajů a omezení jejich uložení. Znamená, že při výkonu sociální politiky by se osobní údaje měli zpracovávat pouze v rozsahu nezbytném a po dobu nezbytnou pro účely zpracování (viz. kapitola 3.4 a 3.6). Každý správce nebo zpracovatel by měl zvážit, zda potřebuje všechny osobní údaje, které zpracovává, zda je potřebuje zpracovávat všemi jím užívanými způsoby a po celou dobu, po kterou je zpracovává. Zároveň by měl zavést mechanizmy, které napomůžou minimalizaci zpracování (při získávání údajů neukládat nepotřebné údaje, nastavit si odpovídající archivační a skartační řád atd.).

4.5. Informovat subjekty údajů o zpracování

Informační povinnost vycházející ze zásady transparentnosti se prolíná celým nařízením GDPR. Nová právní úprava (nikoliv odchylně od původního zákona o ochraně osobních údajů) vyžaduje, aby správce údajů **náležitě informoval jakékoliv dotčené subjekty údajů** o skutečnosti, že jsou jejich osobní údaje zpracovávané. Obsahem informační povinnosti je zejména údaj o tom, které osobní údaje, za jakým účelem a na základě jakého právního titulu jsou zpracovávány, kdo je správcem a případně pověřencem pro ochranu osobních údajů a jaké subjekty nebo kategorie subjektů mohou být příjemci osobních údajů; okruh vyžadovaných informací se lehce liší dle toho, zda správceosobní údaje získá přímo od subjektu údajů (např. od klienta nebo zaměstnance), anebo od třetí osoby (např. od předchozího poskytovatele sociálních služeb); blíže viz čl. 13 a čl. 14 GDPR.

Informační povinnost nevzniká v rozsahu, v jakém subjekt údajů informacemi disponuje. V případě činností pověřených osob určených nezletilým dětem, které odcházejí např. z nějaké akce organizované pověřenou osobou (volnočasové aktivity, hlídání v rámci respitu nabízeného doprovázející organizací atd.) í v doprovodu rodiče nebo jiné kontaktní osoby, musí být této kontaktní osobě zřejmé, že příslušná pověřená osoba o ní zpracovává jisté základní minimum osobních dat (jméno, příjmení, kontaktní údaje) a za jakým účelem tak činí. Subjekt údajů však nemusí mít všechny nezbytné informace (např. týkající se pověřence pro ochranu osobních údajů), a proto lze doporučit, aby v každém případě byla informační povinnost splněna alespoň neadresným způsobem, tj. obecnou informací zveřejněnou na webových stránkách nebo vyvěšenou na nástěnce u vchodu do prostor, kde pověřená osoba působí.

Informace musí být klientovi, zaměstnanci nebo jinému subjektu údajů podávána srozumitelně, stručně a snadno přístupným způsobem za použití „jasných a jednoduchých jazykových prostředků“, viz také kapitola 3.2. To mj. může znamenat, že pro každou kategorii subjektů údajů (klienti, zaměstnanci, dárci) bude informace uvedená na samostatném dokumentu. Obsah a forma informace musí být přizpůsobena adresátovi a jeho rozumovým schopnostem, proto jinak bude vypadat informace určená dospělému a jinak informace určená dítěti nebo mentálně postiženému. Správce nebo zpracovatel musí také posoudit, jaká forma je vhodná pro poskytnutí informace v jeho situaci, tj. zda bude stačit uveřejnění informace na webových stránkách anebo bude informaci poskytovat subjektům údajů (pouze nebo také) individuálně např. v rámci uzavírání smlouvy o poskytování služeb či při získávání souhlasu se zpracováním OÚ. V každém případě by správce nebo zpracovatel měl být schopen splnění informační povinnosti doložit, buď odkazem na zveřejněný dokument nebo obsahem smlouvy či potvrzením subjektu údajů o poskytnutí informace.

4.6. Usnadňovat výkon práv subjektů údajů

Vedle informování subjektů údajů o jejich právech **může** být výkon práv usnadněn také dalšími vhodnými způsoby, jako je **označení kontaktního místa** pro záležitosti ochrany osobních údajů při výkonu sociální politiky na viditelném místě, nebo **vytvoření a zpřístupnění formulářů** pro uplatnění jednotlivých práv, např. formulář na odvolání souhlasu se zpracováním osobních údajů. Důležité je

rovněž zavést u správce údajů procesy a pravidla pro zpracování žádostí subjektů údajů o výkon jednotlivých práv, v rámci kterých by měla být mj. určena osoba odpovědná za vyřízení žádostí subjektů údajů, resp. za rozhodnutí o způsobu vyřízení této žádosti. Faktickou realizaci doporučujeme provést v rámci výše zmíněné interní směrnice správce a případně doplněním popisu pracovních činností dotčených pracovníků podle výstupů dle kapitoly 6.1. v kombinaci s využitím vzorů Příloh č. 5 a 6.

Okruh práv náležejících subjektům údajů se s nařízením GDPR víceméně nemění, pouze přibývá nové právo na přenositelnost údajů, a některá práva, jako právo na výmaz a právo na omezení zpracování, jsou upravena podrobněji, zejména co se týče podmínek pro jejich uplatnění. Nařízení GDPR zná právo na:

1. **přístup k osobním údajům** (tj. na informace o zpracování);
2. **opravu**;
3. **výmaz / „právo být zapomenut“**;
4. **omezení zpracování** (tj. na zdržení se jakéhokoliv zpracování mimo uchování údajů);
5. **přenositelnost osobních údajů** (tj. na vydání zpracovávaných údajů v běžně používaném a strojově čitelném formátu);
6. **námitku** (v případě zpracování OÚ z titulu oprávněných zájmů správce nebo z titulu realizace veřejného zájmu či výkonu veřejné moci, kterým byl správce pověřen – správce si posoudí, zda důvody pro jeho činnost zpracování převažují nad zájmy a právy subjektu údajů, a buď pokračuje se zpracováním, nebo nikoliv);
7. **nebýt předmětem automatizovaného rozhodnutí** (tj. nebýt předmětem rozhodování s právními nebo obdobnými účinky bez účasti lidského faktoru).

Důležité je uvědomit si, že výše uvedená práva subjektů údajů se nemusí dotýkat všech správců a zpracovatelů (např. právo na přenositelnost osobních údajů) a dále, že tato práva nejsou absolutní a uplatnitelná bez výjimky, což bude důležité zejména u práva na výmaz (viz. čl. 17 GDPR) nebo na omezení zpracování (viz. čl. 18 GDPR), případně na právo nebýt předmětem automatizovaného rozhodnutí (viz. čl. 22 GDPR). Žádosti o výmaz osobních údajů tak nebude vyhověno například proto, že správce osobní údaje potřebuje dále pro splnění své zákonné povinnosti, jako je povinnost řádně poskytovat sociální službu nebo povinnost archivovat zdravotnickou dokumentaci, daňové doklady nebo mzdové listy, nebo pro uplatňování právních nároků, např. pro účely vedení soudního sporu.

Jakékoliv úkony a sdělení správce nebo zpracovatele vůči subjektu údajů v souvislosti s realizací jeho práv musí být činěny bezplatně, ledaže je žádost subjektu údajů zjevně nedůvodná nebo nepřiměřená, zejména proto, že se opakuje. V takovém případě může být subjektu údajů uložen přiměřený poplatek za vyhovění žádosti zohledňující administrativní náklady spojené s vyžadovaným úkonem, nebo může být odmítnuto vyhovění žádosti.

4.7. Vést záznamy o činnostech zpracování a správě záznamů

Nově zavedená povinnost vést záznamy o činnostech zpracování v rozsahu dle čl. 30 nařízení GDPR nahrazuje svým charakterem zanikající povinnost předchozí notifikace zpracování osobních údajů Úřadu pro ochranu osobních údajů (nevyžadovala se notifikace zpracování OÚ uloženého zákonem, zpracování veřejně přístupných údajů nebo zpracování v rámci činnosti „sdružení"). Tato povinnost **dopadá víceméně komplexní výkon sociální politiky**, neboť v jeho rámci se zpracovávají osobní údaje systematicky a zpracovávají se také citlivé údaje subjektů údajů.[9]

Záznamy o činnostech zpracování, ať už vedené v papírové nebo elektronické formě (nařízení GDPR stanoví pouze požadavek písemnosti), jsou obecnými záznamy o povaze zpracování u poskytovatele sociálních služeb. Povahově se jedná o jakýsi „krycí list" celé dokumentace poskytovatele k GDPR, který obecně a přehledným způsobem popisuje mj. kategorie zpracovávaných osobních údajů, kategorie dotčených subjektů údajů, účely zpracování, popis zavedených technických a organizačních bezpečnostních opatření (viz. **Příloha č. 3: Vzor – Záznam o činnosti zpracování**).

Záznamy o činnostech zpracování slouží k prokázání souladu zpracování OÚ s GDPR a také jako přehled situace zpracování OÚ pro správce nebo zpracovatele.

Vlastní hodnoty záznamů musí být z důvodu zajištění práv subjektů údajů popsaných v kap. 4.6 vedeny ve vazbě na záznamy o činnostech. Každý záznam, nebo změna hodnoty osobního údaje musí být evidována vzhledem k tomu kdo, kdy, proč a na základě jakého účelu ji provedl. Pro lepší představu lze využít **Přílohu č. 4: Vzor – Záznam zpracování údajů**, který je zpracován pro každý záznam (řádek) v Záznamu o činnostech zpracování.

Je zřejmé, že ve většině případů budou záznamy ukládány v elektronické podobě. Pro nastavení systému stanovuje zmíněná Příloha č. 4 minimální strukturu a obsah logů. Pro listinnou evidenci lze použít Přílohu č. 4, nebo se jí lze inspirovat a doplnit stávající spisovou dokumentaci o chybějící položky. Standardizovaný záznam sociálního pracovníka, nebo zdravotnická dokumentace již požadavek na dokumentaci účelu, adresnosti a datace záznamu obsahují a není třeba je proto z pohledu GDPR upravovat.

Závěrem zdůrazňujeme, že použití záznamů zpracování údajů se primárně týká záznamů vedených v elektronické podobě. V listinné podobě by měly být evidovány záznamy pouze výjimečně a to zejména v případech listin s kritickým obsahem (např. zápůjček soudního spisu apod.)**.**

9 Dle čl. 30 odst. 5 GDPR povinnost vést záznamy o činnostech zpracování dopadá na organizace zaměstnávající 250 a více osob, a dále na subjekty, jejichž zpracování OÚ pravděpodobně představuje riziko pro práva a svobody subjektů údajů, jejichž zpracování není příležitostné, nebo zahrnuje zpracování citlivých údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 GDPR.

4.8. Ohlašovat a oznamovat bezpečnostní incidenty

Nařízení GDPR zavádí nově také povinnost správců údajů **ohlašovat a oznamovat případy porušení zabezpečení osobních údajů**, tedy případy porušení zabezpečení, které vedou k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění osobních údajů – pracovně jsou tyto případy označeny jako tzv. bezpečnostní incidenty. Může se jednat o hackerský útok, jakýkoliv jiný neoprávněný únik údajů, ale i ztráta nezabezpečeného mobilního zařízení zaměstnance s přístupem ke složkám s osobními údaji, ztráta dešifrovacího klíče nebo znehodnocení zdravotnické dokumentace bez existence bezpečnostní zálohy. Bezpečnostními incidenty ve smyslu tohoto materiálu jsou pak incidenty týkající se alespoň částečně osobních údajů, nikoliv incidenty zahrnující pouze jiné druhy dat.

Správce údajů je povinen bez zbytečného odkladu, nejpozději do 72 hodin **poté (!!!), co se o bezpečnostním incidentu dozvěděl, ohlásit tento incident dozorovému úřadu** (viz. Příloha č. 8: Vzor – Ohlašování porušení zabezpečení osobních údajů dozorovému úřadu); případné nedodržení uvedené lhůty musí být odůvodněno. Zdůrazňujeme, že lhůta 72 hodin běží **teprve** od okamžiku protokolárně stvrzeného převzetí informace o bezpečnostním incidentu ze strany správce (např. otevřením podání v datové schránce, písemně stvrzeným převzetím osobního podání, sepsáním protokolu / zápisu o hlášení bezpečnostního incidentu, odesláním potvrzení o doručení emailu, nebo odeslání automatické odpovědi apod.) a je tedy nezbytné v těchto případech instruovat zaměstnance o nezbytnosti uvádět i přesný časový údaj, kdy byla informace převzata. Pokud tedy je hlášení zasláno pouze na email pověřeného zaměstnance, který je na dovolené, běží lhůta od okamžiku, kdy je email doručen, nikoli od času, kdy byl odeslán.

Není-li možné poskytnout dozorovému úřadu všechny vyžadované informace o bezpečnostním incidentu současně, mohou být poskytnuty postupně. Povinnost ohlašování se **netýká případů, kdy je nepravděpodobné, že by incident představoval riziko pro práva a svobody subjektů údajů**, tedy neohlašují se tzv. drobné bezpečnostní incidenty (tím může být např. ztráta bezpečně zašifrovaného mobilního zařízení, chybné založení dokumentu u kterého se nepředpokládá, že se dostal do nepovolaných rukou apod.). Správce údajů je však povinen zdokumentovat všechny, i takovéto, případy v rozsahu, který umožní dozorovému úřadu ověřit, zda poskytovatel postupoval v souladu s GDPR.

Obecně tedy platí povinnost správce každý i nevýznamný bezpečnostní incident vyhodnotit ve lhůtě a pořídit o tom zápis dle vzoru Přílohy č. 8.

Odeslání dozorovému úřadu bude provedeno formou podání prostřednictvím datové schránky, pokud jí správce disponuje. Podání emailem na posta@uoou.cz lze použít pouze jako nouzové opatření a takovéto podání by v souladu s požadavky na zabezpečení osobních údajů nemělo obsahovat konkrétní osobní údaje (ty doporučujeme případně poslat standardní poštou po lhůtě, nebo doručit jiným zabezpečeným způsobem dozorovému úřadu, při využití postupného zasílání informací – viz. výše).

Bezpečnostní incidenty, u nichž je pravděpodobné vysoké riziko pro práva a svobody subjektů údajů, musí být nejenom ohlášeny dozorovému úřadu, ale **rovněž oznámeny dotčeným subjektům údajů**, a to bez zbytečného odkladu (obsah ohlášení je téměř totožný a lze tedy využít vzor dle Přílohy č. 8 s adresací konkrétním subjektům údajů). Vysoké riziko hrozí zejména tehdy, když subjekty údajů můžou dojít, i potenciálně, k nějaké újmě např. z hlediska své psychiky, cti, pověsti či majetku, např. při úniku informací ze zdravotnické dokumentace nebo úniku rozpisů dovolených zaměstnanců společně s jejich soukromými adresami. Oznámení subjektům údajů se nevyžaduje, pokud správce přijal preventivní nebo následná opatření, která zajistí, že se vysoké riziko neprojeví (např. šifrování). **Pokud by oznámení vyžadovalo nepřiměřené úsilí, subjekty údajů mohou být informovány neadresně pomocí veřejného oznámení nebo podobného opatření.**

Také je účelné stanovit, např. ve vnitřní směrnici pro oblast osobních údajů, konkrétní postupy při bezpečnostních incidentech a označit, nejlépe pracovní pozicí a doplněním jejího popisu pracovní činnosti, osoby odpovědné za úkony při plnění těchto povinností, včetně zajištění jejich vzájemné zastupitelnosti, aby nebyly kladeny zbytečné překážky pro začátek lhůty pro vyhodnocování bezpečnostních incidentů.

4.9. Provést posouzení vlivu („DPIA“) a rizik

Novou povinností dle čl. 35 nařízení GDPR je také povinnost **provést posouzení vlivu** zpracování na ochranu OÚ, tzv. DPIA[10], a to v případech, kdy bude pravděpodobné, že určitý druh zpracování, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, přinese vysoké riziko pro práva a svobody subjektů údajů. DPIA ve smyslu čl. 35 GDPR je **specifickým dokumentem**, který se vyžaduje zejména v následujících, v nařízení GDPR uvedených příkladových případech:

(a) systematického a rozsáhlého vyhodnocování osobních aspektů (např. profilování) jako podkladu pro určitá automatizovaná rozhodnutí;

(b) rozsáhlého zpracování citlivých údajů (nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 GDPR); nebo

(c) rozsáhlého systematického monitorování veřejně přístupných prostorů.

Před případným provedením DPIA je tedy potřeba provést základní posouzení rizik (viz. Příloha č. 2: Vzor – Katalog rizik), na základě kterého správce údajů zhodnotí, zda u něj pravděpodobnost vysokého rizika odůvodňuje toto specifické posouzení vlivu na ochranu osobních údajů (DPIA).

Pro zhodnocení nezbytnosti provedení DPIA je nutno konzultovat MPSV, případně vycházet ze seznamu druhů operací zpracování, které dozorový úřad sestaví a zveřejní (čl. 35 odst. 4). Aktuálně byl k 1. 6. 2018 zveřejněn první seznam činností (viz. www.uoou.cz), které nevyžadují posuzování provést (zde je mj. explicitně zmíněno zpracování zajišťovaná jednotlivými podnikajícími fyzickými osobami poskytujícími sociální služby).

10 Posouzení vlivu na ochranu OÚ (DPIA) je postup, jehož záměrem je popis zpracování OÚ, posouzení jeho nezbytnosti a přiměřenosti a posouzení rizik zpracování pro práva a svobody subjektů údajů a stanovení opatření k jejich řešení.

Pokud se správce rozhodne posouzení vlivu provést, mělo by obsahovat minimálně:

1. systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce (informační aktiva – proces);
2. posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů (legislativní povinnost);
3. posouzení rizik pro práva a svobody subjektů údajů;
4. plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Lze konstatovat, že uvedené minimum provede správce, pokud bude postupovat v souladu s kapitolou 5, konkrétně pak:

Ad1 a 2) zpracováním katalogu osobních údajů

Ad3 a 4) zpracováním analýzy rizik jednotlivých záznamů v katalogu osobních údajů a zpracováním návrhů nápravných opatření

DPIA by mělo být provedeno **„před zpracováním“**, ale je dovozováno, že tato povinnost by měla být splněna nikoliv pouze ohledně budoucích, zamýšlených zpracování, ale také ohledně stávajících zpracování OÚ (tj. zpracování před účinností GDPR), ovšem pokud u nich již posouzení neproběhlo nebo tato nebyla konzultována s ÚOOÚ. Posouzení vlivu na ochranu OÚ je navíc neustálý, a nikoliv jednorázový proces – posouzení je potřeba průběžně aktualizovat. Tato povinnost bude splněna a kontrolována v rámci auditního procesu (kap. 7), který předpokládá aktualizaci a revizi záznamů (viz. bod 2 kap. 7) a kontrolu a případně revizi úrovně řízení rizik (viz. bod 3 kap. 7).

Pokud správce údajů na základě DPIA dospěje k závěru, že nemá k dispozici dostatečná opatření ke snížení rizika na přijatelnou míru, tj. *zbytková rizika zůstávají vysoká*, je nutná **konzultace s dozorovým úřadem**. Nelze vyloučit, že v závažných případech dozorový úřad určité způsoby zpracování OÚ zakáže.

Kromě uvedeného je konzultace s dozorovým úřadem nezbytná také tehdy, když *právo členského státu uloží* správci *povinnost* konzultovat s dozorovým úřadem anebo získat od něj předchozí povolení, pokud jde o zpracování OÚ za účelem vykonání úkolu ve veřejném zájmu, včetně zpracování v souvislosti se sociální ochranou a veřejným zdravím (čl. 36 odst. 5 GDPR). **Zatím taková povinnost z právních předpisů ČR nevyplývá.**

Závěrem zdůrazňujeme, že v případě nezbytných konzultací s dozorovým úřadem se jedná o výjimečné případy, které při výkonu sociální politiky neočekáváme a doporučujeme v případě pochybností primárně kontaktovat MPSV ke konzultaci.

4.10. Jmenovat pověřence pro ochranu osobních údajů

V případě, že správce nebo zpracovatel je povinen ustanovit pověřence pro ochranu osobních údajů, anebo se rozhodne ustanovit ho dobrovolně, je potřeba pamatovat na to, aby pověřencem byla vybrána osoba disponující potřebnými znalostmi a praxí v oblasti ochrany osobních údajů a aby tato osoba detailně znala, příp. byla detailně seznámena se systémem zpracování osobních údajů „svého" správce. Pověřenec může vykonávat funkci z pozice zaměstnance poskytovatele sociálních služeb, anebo jako externí poskytovatel služeb; je ovšem nezbytné zajistit, aby u něj **nedocházelo ke střetu zájmů**, zejména vykonává-li u správce ještě další činnost a musí mít dostatečný pracovní prostor k provádění činností souvisejících s ochranou osobních údajů ve smyslu požadavků GDPR.

Pověřencem by tedy neměla být ustanovena osoba, která se poskytovatele nějakým zásadním způsobem podílí na zpracování osobních údajů (může rozhodovat o účelech a prostředcích zpracování) **a/nebo je statutárním zástupcem orgánem či vedoucím pracovníkem správce** (např. vedoucí HR nebo IT pracovník, ředitel nebo jiná vedoucí osoba rozhodující o otázkách zpracování OÚ). Pokud by poskytovateli službu pověřence poskytovala právnická osoba, doporučuje se smluvně ji zavázat, aby při výběru fyzické osoby odpovědné za výkon funkce pověřence dodržela kritéria zde vymezená.

Nařízení GDPR zdůrazňuje **nezávislý výkon** funkce pověřence, který **nesmí ohledně výkonu této funkce dostávat žádné pokyny** (mohou mu být zadávány úkoly, nicméně neměl by dostávat pokyny ohledně způsobu jejich vyřízení) a nesmí být za výkon své funkce sankcionován. Poskytovatel sociálních služeb zajistí, aby byl pověřenec náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů, aby měl přístup k osobním údajům a operacím zpracování, a poskytne mu zdroje nezbytné k plnění jeho funkce a k udržování jeho odborných znalostí. Pověřenec by měl mít **přímý přístup k vedení** poskytovatele sociálních služeb, aby se na vedení organizace mohl kdykoli obrátit v záležitostech ochrany osobních údajů. Je-li pověřenec jmenován, správce zveřejní jeho kontaktní údaje a zároveň je sdělí dozorovému úřadu (forma sdělení údajů dozorovému úřadu nebyla dosud stanovena, předpokládá se standardním dopisem).

Nařízení GDPR umožňuje, aby několik správců (poskytovatelů sociálních služeb) jmenovalo **společného pověřence**, musí být však snadno dosažitelný z každé organizace, pro kterou je činný.

V případě, že se poskytovatel sociálních služeb rozhodne pověřence pro ochranu osobních údajů nejmenovat, doporučuje se, aby vypracoval **interní analýzu** popisující provedené posouzení, aby byl schopen prokázat, že byly řádně zohledněny relevantní faktory. Tato analýza je součástí dokumentace podle zásady odpovědnosti správce (dokládající soulad s GDPR).

Závěrem je důležité upozornit, že **i v případě, kdy je pověřenec jmenován, odpovědnost za zákonnost a správnost postupů zpracování osobních údajů nese dále správce**.

5. ANALÝZA STÁVAJÍCÍHO STAVU OÚ A JEJICH RIZIK

Před zahájením vlastní implementace GPDR je nezbytné provést základní analýzu stavu organizace a identifikovat všechny zpracovávané osobní údaje a rizika s nimi spojená. Tato činnost je základem, který umožňuje identifikovat všechny dotčené procesy uvnitř organizace a odůvodnit jejich účelnost.

Zároveň důrazně doporučujeme stanovit minimálně jednoho pracovníka, který se bude problematikou osobních údajů zabývat a bude spolupracovat se subjekty údajů, zpracovateli, pověřencem (pokud byl jmenován) a dozorovým úřadem. Rozsah činností, kterými se bude zabývat, vychází z velikosti organizace a množství zpracovávaných sad údajů (u malé organizace se může jednat o cca 8 hodin měsíčně, u velké se může jednat až o plný pracovní úvazek).

5.1. Analýza stávajícího stavu

Hlavním výstupem analýzy stávajícího stavu bude vyplněná Příloha č. 1: Vzor – Katalog osobních údajů. Tento dokument je nejvýznamnější součástí řešení problematiky osobních údajů, protože stanovuje základní rámec zpracování konkrétních sad osobních údajů, odůvodňuje účel tohoto zpracování a konečně stanovuje osoby odpovědné za zpracování, nebo přístup k těmto OÚ.

Vlastní zpracování je nezbytné provést velmi důkladně, ideálně se zapojením všech zaměstnanců a dodavatelů. Časová náročnost se při zapojení širokého okruhu pracovníků pohybuje na 1-2 hodinách zúčastněných a to včetně základního školení na vyplnění dokumentu a včetně doplňujících dotazů.

Pro zjištění všech údajů doporučujeme postupovat prostřednictvím tzv. prohlídek. Tento systém umožňuje dostupnější formou realizovat procesní analýzu organizace, která je de facto pro potřeby analýzy stávajícího stavu požadována.

Pro zjištění všech zpracovávaných osobních údajů doporučujeme provedení:

1. Fyzické prohlídky, která obsahuje identifikaci osobních údajů v:
    a. dokumentaci poskytovatele (interní dokumenty, směrnice, nařízení, zakládací listiny)
    b. dokumentaci klientů (spisové materiály, poznámky, interní hodnocení)
    c. dokumentaci zaměstnanců (personální složky, pracovní složky, organigramy)
    d. dodavatelsko-odběratelských vztazích (smlouvách, dokumentech i plnění)
    e. obrazových i audiovizuálních materiálech (v tištěné i elektronické podobě)
    f. prostorách, kde je vykonávána činnost poskytovatele (nástěnky, tabule, informační lístky, identifikační karty apod.)
    g. ostatních dokumentech a záznamech (např. evidence úrazů, pravidelné revize, tzv. pomocné evidence zaměstnanců apod.)

2. Elektronické prohlídky, která řeší identifikaci osobních údajů v:
    a. dokumentech v elektronické formě
    b. databázových strukturách
    c. interních aplikacích
    d. externích aplikacích a službách
    e. virtuálních úložištích

3. Příkladová prohlídka, která aplikací sady zkoumaných příkladů (obsahující většinu činností poskytovatele) nahrazuje částečně intuitivní formou procesní analýzu a doplňuje a kontroluje výstupy získané v předchozích krocích. Sada zkoumaných příkladů by měla minimálně obsahovat příklad pro:
    a. každou poskytovanou službu (především sociální službu, nebo její ekvivalent SPOD)
    b. komunikaci s třetími stranami (zejména se týká krajů, MPSV, veřejné správy, ostatních subjektů vykonávajících sociální politiku apod.)
    c. každou interní skupinu agend, nebo agendu (personalistiku, účetnictví, dodavatelsko-odběratelské vztahy, apod.)
    d. vnější prezentaci organizace (www stránky, marketing, propagaci organizace apod.)

Součástí prohlídek dokumentace by mělo být i přehodnocení stávající dokumentace práce s osobními údaji, především v kontextu jejich použitelnosti a souladu s nařízením GDPR.

Zejména v případě elektronické prohlídky je zásadní spolupráce s konkrétními zaměstnanci a dodavateli. Část údajů se totiž může nacházet v privátních složkách, ke kterým zaměstnavatel nemá přístup a je nezbytné požádat zaměstnance o jejich kontrolu. Také v případě externích služeb (např. ve formě vzdáleného serveru, nebo cloudového úložiště) nelze z pozice uživatele stanovit přesné umístění a vyhodnotit související rizika (viz. kap. 5.2) a dokonce ani zajistit, že místo, kde jsou uloženy osobní údaje je v jurisdikci nařízení GDPR. V těchto případech, kdy nelze zajistit splnění nařízení je jediným možným postupem takovouto službu, nebo aplikaci nahradit jiným řešením.

Výstupem provedených prohlídek je tedy katalog osobních údajů, který obsahuje minimálně pro každý případ:

1. specifikaci identifikovaných osobních údajů
2. oblast subjektu údajů
3. proces / činnost, ve kterém jsou údaje zpracovávány
4. evidenci / aplikaci / službu, která s nimi pracuje
5. gestora a uživatele oprávněné s nimi nakládat
6. umístění osobních údajů (fyzické i virtuální)
7. oprávnění jejich zpracování
8. délku zpracování a archivační / skartační lhůty

5.2. Analýza rizik

Analýza rizik je obecně základním nástrojem pro udržování systémů řízení kvality v chodu a v minimalizaci dopadů mimořádných událostí na stav organizace. Teoreticky by každá organizace měla analýzu rizik a s ní spojený management rizik provádět. Většina organizací se ale spokojí s její intuitivní podobou (většinou řešenou statutárem, nebo členy vedení, kteří se snaží rizika obecně identifikovat a eliminovat) a formální evidenci vedou pouze v případech vyžadovaných zákonem (např. BOZP, revize vybavení, kybernetická bezpečnost apod.). Bohužel implementace nařízení GDPR takovouto formální analýzu rizik a na ní návazný management vyžaduje (viz. Příloha č. 2: Vzor – Katalog rizik).

Analýza rizik osobních údajů přímo navazuje na vytvoření katalogu osobních údajů v kap. 5.1. Analýzu rizik provede organizace minimálně ve formě Přílohy č. 2 **pro každý záznam (tj. řádek) katalogu osobních údajů**. Je zřejmé, že velká část rizik se při tomto přístupu bude opakovat a je tedy možné rizika slučovat a odkazovat je na identifikátory v katalogu osobních údajů.

Identifikace rizik by měla obsahovat komplexní soubor všech hrozeb posuzované sadě osobních údajů, tj. minimálně posouzení:

1. **oprávněnosti** – zda je mohu zpracovávat (čl. 25)
2. **dostupnosti** – kdo s nimi pracuje (čl. 25)
3. **bezpečnosti** – jak jsou zabezpečena (čl. 32)
4. **logování** – tj. hodnocení úrovně dokumentace zpracování (čl. 30)
5. **přístupnosti** – možnosti přístupu, oprav a mazání ze strany subjektu údajů (čl. 14 – 19)
6. **rizikovosti** pro práva a svobody subjektu (čl. 35)

Po identifikaci je nezbytné riziko v souladu s Přílohou č. 2 popsat a především navrhnout nápravné opatření, které bude minimalizovat závažnost a pravděpodobnost rizika, nebo jej ideálně úplně eliminovat. Nápravná opatření mohou být několikastupňová (od provizorních a dočasných, až po komplexní a trvalá, která ovlivňují chod celé organizace). Důležité je především při návrhu zohledňovat možnosti a potřeby organizace a tedy zohledňovat jak kapacitní, tak finanční rámce navržených řešení.

Obsahově se může jednat o opatření fyzické, administrativní, personální, technické, nebo dokumentační. Opatření může být vztaženo k riziku i skupině rizik, stejně jako může být definováno k jednomu riziku více opatření. Při formulaci nápravného opatření, pokud není jasné, jak riziko řešit doporučujeme konzultovat s pověřencem, KÚ, MPSV, nebo dozorovým úřadem.

Výstupem těchto činností je tedy katalog rizik s navrženými nápravnými opatřeními. Management rizik, tj. práce s identifikovanými záznamy, spočívá v jednoduchém cyklu realizace nápravných opatření: formulace nápravných opatření – jejich zavedení do praxe – vyhodnocení jejich efektu – revize rizika, resp. nová analýza rizik – formulace nápravných opatření – atd.

Uvedený proces je nezbytné provádět opakovaně a pravidelně, protože stav identifikovaných rizik je důležitým podkladem pro vyhodnocení bezpečnostního incidentu a případné ohlašovací povinnosti směrem k dozorovému úřadu.

6. IMPLEMENTACE SYSTÉMU GDPR

Pro zajištění souladu s nařízením GDPR je nezbytné naplnit tři základní cíle organizace:

1. schopnost poskytnout informace a součinnost subjektu údajů
2. odůvodnit existenci konkrétních dat u správce a dokumentovat operace s nimi spojené
3. obhájit postup zpracování a úroveň zabezpečení osobních údajů

Realizaci těchto cílů umožňujících nalezení optimální a co nejjednodušší cesty k souladu s nařízením GDPR jsme pro přehlednost rozdělili také na tři části:

1. Definovat a implementovat / upravit procesy vztahující se k GDPR
2. Definovat a implementovat nápravná opatření z Katalogu rizik
3. Zavést a průběžně aktualizovat řízenou dokumentaci

Jednotlivé části implementace podrobně popíšeme v následujících kapitolách.

6.1. Procesy GDPR

Nařízení GDPR nově zavádí některé povinnosti, které musí být realizovány samostatnými, nebo různě upravenými stávajícími procesy v organizaci. Tyto změny vyplývají především z nově zavedené povinnosti dokladovat soulad s nařízením GDPR správcem osobních údajů.

Hlavním procesem je zde proces sběru, vyhodnocení a ohlášení bezpečnostních incidentů souvisejících s riziky pro práva a svobody fyzických osob. V rámci tohoto procesu je nezbytné definovat jednotlivé činnosti a přiřadit jim konkrétní účastníky. Postup sběru je reakcí organizace na standardní podání, ale s označením urgence, vzhledem k 72 hodinové lhůtě na jeho vypořádání a případné ohlášení dozorovému úřadu. Postup vyhodnocení vyplývá z obsahu Přílohy č. 7: Vzor – Identifikace porušení zabezpečení a posouzení rizika pro práva a svobody fyzických osob a při použití tohoto vzoru stačí organizaci zajistit přidělení vyhodnocení kompetentnímu pracovníkovi. Vlastní případné ohlášení je pouze standardním vypravením podání dozorovému úřadu (např. prostřednictvím datové schránky).

Proces komunikace se subjekty údajů je obdobný a při použití citace z nařízení GDPR a stanovení kompetentní osoby jej lze redukovat na standardní agendu přijetí a zpracování podání a vypravení odpovědi.

V některých organizacích nově vzniknou procesy spojené s managementem rizik popsaným v kap. 5.2 a zpracováním katalogu osobních údajů (viz. kap. 5.1) spojeným s definicí účelu zpracování.

Obecně lze také očekávat individuální požadavky na formalizaci postupů a nakládání s osobními údaji v závislosti na úrovni technického vybavení a množství agend řešených jednotlivými organizacemi.

6.2. Nápravná opatření

Seznam nápravných opatření určených k realizaci bude v případě úvodní implementace vycházet z analýzy stávajícího stavu a navazující analýzy rizik. Soubor těchto opatření lze rozdělit na úpravy stávající dokumentace (nová dokumentace bude zavedena v kap. 6.3) a technická opatření.

Mezi základní úpravy stávající dokumentace patří:

1. úpravy pracovních činností zaměstnanců s ohledem na GDPR
2. zajištění shody záznamů obsahujících osobní údaje s nařízením GDPR
3. doplnění smluvních ustanovení (dle vzorů v budoucnu zveřejněných dozorovým úřadem)
4. úpravy formy poskytovaných souhlasů dle pravidel v kap. 4
5. úprava formy (doplnění) informací poskytovaných subjektům údajů

Mezi nejčastěji využívaná technická opatření patří:

1. doplnění vnitřních funkcí informačních systémů (logování, šifrování, pseudonymizace apod.), které ale řeší dodavatelé těchto systémů často z vlastní iniciativy, takže postačuje aktualizace používaných SW na verze vydané po 25. 5. 2018
2. používání uživatelských pravidel (definice uživatelských rolí a jejich oprávnění přístupu k datům i ke konkrétním prostředkům)
3. fyzická opatření (omezení neoprávněných přístupů, systém udělování oprávnění, klíčové hospodářství, zabezpečení vybraných prostor apod.)
4. zavedení bezpečnostních politik (jak obecných, tak podle zákona o kybernetické bezpečnosti)

Tuto fázi implementace GDPR lze považovat za ukončenou v okamžiku, kdy realizovaná nápravná opatření eliminují rizika nesouladu s nařízením GDPR v analýze rizik.

6.3. Řízená dokumentace GDPR

Řízenou dokumentací rozumíme pro potřeby tohoto kodexu soubor dokumentů s řízenou publikací a sledováním změn. Jednotlivé verze dokumentů jsou vydávány buď v pravidelných časových intervalech (např. jednou ročně), nebo jako důsledek vybrané události (vyhodnocení bezpečnostního incidentu, interní audit, doporučení dozorového úřadu, apod.).

Základní sada dokumentu nezbytných pro zajištění souladu s nařízením GDPR obsahuje:

1. **Interní směrnici organizace** – interní dokument, kterým se zejména správce přihlašuje ke kodexu chování a zavazuje svoje zaměstnance a spolupracující subjekty dodržováním nařízení GDPR
2. **Kodex chování** – zde ve formě doporučeného metodického postupu, který bude řízen a aktualizován MPSV
3. **Záznamy o činnostech zpracování** – dokument dle čl. 30 viz. Příloha č. 3: Vzor – Záznam o činnostech zpracování
4. **Záznamy o zpracování** – dokument/datový soubor obsahující evidence všech přístupů k osobním údajům a operací s nimi spojenými (viz. Příloha č. 4: Vzor – Záznam zpracování údajů). Zdůrazňujeme, že vzorový dokument slouží pouze jako nouzové řešení evidence práce se záznamy a je preferováno elektronické a ideálně automatické logování činností.
5. **Záznam o komunikaci se subjektem údajů** – evidence korespondence, postačuje řešit formou systematického používání spisové služby
6. **Záznamy o posouzení** – viz. Příloha č. 7: Vzor – Identifikace porušení zabezpečení a posouzení rizika pro práva a svobody fyzických osob
7. **Evidence procesu identifikace bezpečnostních incidentů** – shodně s bodem 5
8. **Ohlašování porušení zabezpečení osobních údajů dozorovému úřadu** – viz. Příloha č. 9

7. AUDIT SYSTÉMU GDPR

Auditní činnost prováděná v systému výkonu sociální politiky bude podrobně zpracována po ustálení výkladové praxe a především po ustavení dozorového úřadu, který bude mít kompetenci vydávat podmínky udělení osvědčení pro ochranu osobních údajů a zavádění pečetí a známek dokladujících ochranu údajů pro účely prokázání souladu s nařízením GDPR.

Proto nyní uvedeme pouze několik obecných pravidel a činností, které by měl interní audit správce, nebo jeho metodického orgánu obsahovat.

Auditor by zejména měl klást důraz na:

1. zhodnocení systému zpracování osobních údajů jako celku,
2. stav a úroveň řízené dokumentace (aktuálnost, dostupnost, seznámení uživatelů s jejím obsahem apod.)
3. úroveň řízení rizik, především z pohledu pravidelnosti aktualizace stavu rizik správce a vyhodnocování dopadu přijatých nápravných opatření,
4. stav dostupnosti a bezpečnosti vlastních záznamů, včetně záznamů o jejich prohlížení a změnách,
5. vyhodnocení činnosti pověřence a jeho součinnosti se správcem,
6. posouzení kontrolních mechanizmů systému jako celku.

8. SEZNAM PŘÍLOH

Příloha č. 1: Vzor – Katalog osobních údajů
Příloha č. 2: Vzor – Katalog rizik
Příloha č. 3: Vzor – Záznam o činnostech zpracování
Příloha č. 4: Vzor – Záznam zpracování údajů
Příloha č. 5: Vzor – Poskytnutí přístupu k osobním údajům
Příloha č. 6: Vzor – Oznamovací povinnost o změně osobních údajů
Příloha č. 7: Vzor – Identifikace porušení zabezpečení a posouzení rizika pro práva a svobody fyzických osob
Příloha č. 8: Vzor – Ohlašování porušení zabezpečení osobních údajů dozorovému úřadu
Příloha č. 9: Vzor – Posouzení vlivu na ochranu osobních údajů