Směrnice o zpracování osobních údajů

vydaná dne 25. 5. 2018

SHRNUTÍ

Účelem této směrnice je poskytnutí pravidel pro nakládání s osobními údaji a s dokumenty obsahujícími tyto osobní údaje. Součástí je také obecný návod, jak jednat v souladu s organizačně-technickými a dalšími opatřeními směřujícími k dodržení platných a účinných právních předpisů na ochranu osobních údajů v rámci **Mateřské školy Praha 9 – Černý Most, Paculova 1115**, **příspěvková organizace**, správce **Mgr. Andrea Benešová**. („**Správce**“)

Směrnice mezi jinými určuje účel a rozsah shromažďování a zpracování osobních údajů, prostředky a způsob jejich zpracování, jakož i práva a povinnosti osob ve vztahu k těmto údajům a zacházení s nimi. Chránit osobní údaje je povinností jak Správce, tak každého jeho pracovníka. Konkrétní pravidla související s dílčími druhy zpracování osobních údajů (jako zpracování zaměstnaneckých dat, či údajů třetích osob) obsahují jednotlivé *Záznamy o činnostech zpracování osobních údajů (čl. 30 GDPR)*, přičemž ve spojení se Směrnicí jsou tak pracovníkům Správce nastavena pravidla a možnosti zpracování osobních údajů. Není- li odpovědnost při stanovení konkrétní povinnosti v textu dále uvedena, za její zajištění je odpovědný ředitel, resp. ředitelka Správce.

Směrnice je interním normativním předpisem, který zavazuje všechny zaměstnance, další pracovníky a spolupracující osoby Správce, jakož i další osoby, jež podléhají interním předpisům Správce, stejně jako osoby, jež se k dodržování této Směrnice zavázaly v rámci smluvního vztahu se Správcem nebo se zpracovatelem.

ZÁKLADNÍ PRINCIPY

Správce a všichni jeho pracovníci jsou při nakládání s osobními údaji povinni dodržovat GDPR a národní prováděcí právní úpravu (viz *článek 1.1*). Především GDPR stanoví hlavní pravidla a zásady, kterými je potřeba se při zpracování osobních údajů řídit, a Správce tyto zásady přebírá.

ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. **Zákonnost, korektnost a transparentnost:** Veškeré osobní údaje zpracovávané Správcem musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem;
2. **Účelové omezení:** Osobní údaje lze shromažďovat pouze pro určité, výslovně vyjádřené a legitimní účely a tyto údaje nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;
3. **Minimalizace údajů:** Osobní údaje lze zpracovávat pouze v rozsahu nezbytném pro naplnění stanoveného účelu;
4. **Přesnost:** Zpracovávat lze pouze přesné a v případě potřeby aktualizované osobní údaje; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny;
5. **Omezení uložení:** Uchovávat osobní údaje ve formě umožňující identifikaci subjektů údajů lze pouze po dobu ne delší, než je nezbytné pro účely zpracování;
6. **Integrita a důvěrnost:** Osobní údaje lze zpracovávat pouze způsobem, který zajistí náležitou ochranu osobních údajů pomocí vhodných technických nebo organizačních opatření, a to před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením;

7. **Odpovědnost:** Dodržení výše uvedených zásad včetně souladu s platnými a účinnými právními předpisy na ochranu osobních údajů musí být Správce schopen doložit;

8. **Přístup založený na míře rizika (tzv. Risk Based Approach)**: Čím větší je riziko, že daný druh zpracování prováděný Správcem může zasahovat do zájmů či základních práv a svobod subjektu údajů, tím vyšší opatření vedoucí k transparentnosti a bezpečnosti daného zpracování je třeba přijmout. Není-li si daný pracovník, který nakládá s osobními údaji, jistý, jaké riziko je s daným zpracováním spojeno, či jaké konkrétní povinnosti se na něj v souvislosti se zpracováním osobních údajů vztahují, obrátí se na osobu odpovědnou za zpracování osobních údajů Správce nebo následně s jeho vědomím na pověřence pro ochranu osobních údajů.

KONKRÉTNÍ PRAVIDLA

1. ZÁKLADNÍ USTANOVENÍ

1.1 Práva a povinnosti Správce při shromažďování, uchovávání a zpracování osobních údajů jsou stanoveny především Nařízením 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) („**Nařízení**“ nebo „**GDPR**“) a prováděcí národní legislativou, jak bude přijata („**Zákon**“).

1.2 Tato směrnice o zpracování osobních údajů („**Směrnice**“) stanoví zejména:

i) zásady zpracování osobních údajů;

ii) jmenování osoby odpovědné za ochranu osobních údajů u Správce, její postavení a pravomoci;

iii) účel a rozsah shromažďování osobních údajů;

iv) prostředky a způsob zpracování osobních údajů;

v) pravidla pro zapojení zpracovatele a náležitosti smlouvy o zpracování uzavírané mezi Správcem a zpracovatelem osobních údajů;

vi) práva a povinnosti konkrétních osob ve vztahu k osobním údajům a zacházení s nimi;

vii) pravidla zpracování zvláštních kategorií osobních údajů;

viii) postup pro získání platného souhlasu a hlavní zásady vztahující se k jeho legitimitě;

ix) způsob plnění informační povinnosti;

x) procesy reakce a vypořádání se s právy subjektu údajů; a

xi) postupy hlášení případů porušení zabezpečení osobních údajů.

1.3 Dále Směrnice stanoví organizačně-technická a další opatření směřující k zajištění dodržování Nařízení a Zákona, a to zejména čl. 32 Nařízení, při nakládání s osobními údaji v podmínkách Správce. Směrnice mezi jinými určuje účel a rozsah shromažďování a zpracování osobních údajů, prostředky a způsob jejich zpracování, jakož i práva a povinnosti osob ve vztahu k těmto údajům a zacházení s nimi.

1.4 Správce je povinen vynaložit přiměřené úsilí, aby se osoby, které zpracovávají osobní údaje na základě smlouvy s ním, se zavázaly dodržovat ustanovení této Směrnice.

1.5 Pokud text v této Směrnici odkazuje na jiná ustanovení (články, položky), rozumí se tím příslušná ustanovení této Směrnice, není-li v daném případě výslovně uvedeno jinak.

2. ZÁKLADNÍ POJMY

V souladu s Nařízením a Zákonem se pro účely této Směrnice rozumí:

Osoby nakládající s osobními údaji a subjekt údajů

(a) **správcem** subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů nebo kterému povinnost zpracovávat osobní údaje ukládají platné a účinné právní předpisy;

(b) **zpracovatelem** fyzická nebo právnická osoba, orgán veřejné moci, nebo jiný subjekt, který zpracovává osobní údaje pro správce; blíže jeho postavení vymezuje *článek 7*;

(c) **subjektem údajů** identifikovaná nebo identifikovatelná živá fyzická osoba (nikoliv osoba právnická a nikoli osoba zemřelá). Subjekty údajů pro účely této Směrnice jsou osoby uvedené v *položce Kategorie subjektů údajů v Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)*;

(d) **příjemcem** fyzická nebo právnická osoba, orgán veřejné moci nebo jiný subjekt, kterému jsou osobní údaje poskytnuty (s výjimkou orgánů veřejné moci, které mohou získávat osobní údaje na základě platných a účinných právních předpisů); kategorie příjemců jsou uvedeny v *Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)*;

Osobní údaje a kategorie osobních údajů

(e) **osobním údajem** veškeré informace subjektu údajů, který lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, datum narození, identifikační číslo, adresní a kontaktní údaje, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity; za osobní údaje se považují i údaje, které se samy o sobě netýkají fyzické osoby, ale ve spojení s jinými informacemi by již bylo alespoň potenciálně možné tyto údaje přiřadit ke konkrétní fyzické osobě (např. barva a značka osobního vozidla, jako údaje týkající se věci, která sama o sobě nesouvisí s fyzickou osobou);

(f) **zvláštní kategorií osobních údajů** osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby; zvláštní ochrany požívají údaje týkající se odsouzení za trestné činy;

(g) **biometrickými údaji** osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

(h) **anonymním údajem** takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů – nejedná se tedy o osobní údaj;

Zpracování osobních údajů

(i) **zpracováním 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, ale i výmaz nebo zničení;

(j) **shromažďováním osobních údajů** systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování;

(k) **uchováváním osobních údajů** udržování údajů v takové podobě, která je umožňuje dále zpracovávat;

(l) **likvidací osobních údajů** fyzické zničení jejich nosiče, jejich fyzické vymazání nebo trvalé vyloučení z dalších zpracování; formou likvidace osobních údajů je i **anonymizace**;

(m) **anonymizací** činnost, při které dojde k trvalému smazání či rozpojení identifikátorů, pomocí kterých je možné ztotožnit konkrétní fyzickou osobu;

(n) **pseudonymizací** 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 fyzické osobě; po opětovném přiřazení dodatečných informací je možné konkrétní fyzickou osobu opětovně identifikovat;

(o) **profilováním** jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se např. jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu apod.;

Další

(p) **souhlasem subjektu údajů** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

(q) **databází/evidencí** jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

(r) **popisem databáze**[1] vymezení jednotlivých databází v *Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)* („**příslušný popis databáze**“);

(s) **porušením zabezpečení osobních údajů** (tzv. „**Data Breach**“) porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

3. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

3.1 Správce jmenoval pověřence osobních údajů („**DPO**“), který dohlíží na dodržování ochrany **osobních údajů** u Správce. Kontaktní údaje na DPO jsou uvedeny v Poučení subjektů o zpracování osobních údajů, které tvoří nedílnou součást této Směrnice (Příloha č. 2 Poučení subjektů o zpracování osobních údajů).

3.2 DPO je hlavním garantem dodržování Nařízení, Zákona a této Směrnice ze strany zaměstnanců Správce, jakož i dalších osob uvedených v *článku* ***Chyba! Nenalezen zdroj odkazů.***.

3.3 DPO poskytuje informace a poradenství všem zaměstnancům Správce, jakož i dalším osobám uvedených v *článku* ***Chyba! Nenalezen zdroj odkazů.***, kteří provádějí zpracování, o jejich povinnostech podle Nařízení, Zákona a této Směrnice.

3.4 DPO musí být vedením Správce, jakož i zaměstnanci konzultován ve všech zásadních otázkách týkajících se zpracování a/nebo ochrany osobních údajů a musí být zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.

3.5 DPO monitoruje soulad s Nařízením, Zákonem a touto Směrnicí, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků Správce zapojených do operací zpracování a souvisejících auditů.

3.6 DPO poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů (viz *článek 17*), a monitorování jeho uplatňování podle čl. 35 Nařízení.

3.7 DPO komunikuje a spolupracuje jménem Správce s Úřadem pro ochranu osobních údajů („**ÚOOÚ**“) a zejména zajišťuje jménem Správce veškerá příslušná podání k ÚOOÚ. Především se jedná o předchozí konzultaci dle čl. 36 Nařízení a předávání osobních údajů do zahraničí podle čl. 44 a násl. Nařízení.

3.8 DPO je odpovědný za udržování příslušných popisů databází, které aktualizuje vždy s ohledem na posouzení rizik souvisejících se zpracováním osobních údajů podle čl. 32 Nařízení.

[1] Pojem s významem pro účely této Směrnice.

3.9 Osoby vázané touto Směrnicí jsou povinny DPO informovat o veškerých skutečnostech, které mohou být významné pro ochranu osobních údajů ze strany Správce.

3.10 DPO plní i další povinnosti stanovené jemu touto Směrnicí.

4. ÚČEL A ROZSAH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

4.1 Správce shromažďuje a zpracovává osobní údaje za účely stanovenými v *Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)*.

4.2 Zpracování osobních údajů nesmí přesáhnout míru nezbytnou k dosažení účelu zpracování v konkrétním případě.

4.3 Zpracovávány mohou být v zásadě pouze osobní údaje stanovené v položce Kategorie zpracovávaných osobních údajů *Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)*.

4.4 Zpracování zvláštních kategorií osobních údajů je možné bez souhlasu subjektu osobních údajů pouze v případě, že tak výslovně stanoví příslušné právní předpisy nebo dále z důvodů čl. 9 odst. 2 Nařízení. V opačném případě musí být jakýkoliv osobní údaj zvláštní kategorie anonymizován nebo zlikvidován.

4.5 Osobní údaje mohou být Správcem předávány nebo zpřístupněny na základě zákona příslušným státním orgánům a dalším osobám, jež upravují zvláštní právní předpisy (např. Policie ČR), nebo dalším správcům, kteří zpracovávají předávané osobní údaje bez souhlasu subjektu údajů na základě zákonného důvodu. Osobní údaje mohou být Správcem předávány dalším osobám také na základě souhlasu subjektu údajů nebo jiného zákonného důvodu.

4.6 Osobní údaje mohou být uchovávány pouze po dobu nezbytnou k dosažení účelu zpracování, resp. po dobu uvedenou v *položce Plánovaná doba uchování osobních údajů Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)* anebo po dobu uvedenou ve *skartačním řádu*. Po uplynutí této doby je třeba provést likvidaci osobních údajů v souladu s *článkem 16*.

5. ŠKOLNÍ MATRIKA

5.1 Zvláštní důraz na ochranu osobních údajů Správce klade v agendě školní matriky, kdy způsob zpracování a vedení školní matriky se řídí zákonem č. 561/2004 Sb., školský zákon a vyhláškou č. 364/2005 Sb., o dokumentaci škol a školských zařízení, obojí ve znění pozdějších předpisů.

5.2 Správce v rámci školní matriky zpracovává v souladu se školským zákonem následující údaje:

(a) jméno a příjmení, rodné číslo, popřípadě datum narození, nebylo-li rodné číslo dítěti přiděleno, dále státní občanství, místo narození a místo trvalého pobytu, popřípadě místo pobytu na území České republiky podle druhu pobytu cizince nebo místo pobytu v zahraničí, nepobývá-li dítě na území České republiky,

(b) datum zahájení vzdělávání ve škole,

(c) údaje o průběhu a výsledcích vzdělávání ve škole, vyučovací jazyk,

(d) údaje o znevýhodnění dítěte, žáka nebo studenta uvedeném v § 16 školského zákona, údaje o mimořádném nadání, údaje o podpůrných opatřeních poskytovaných dítěti, žákovi nebo studentovi školou v souladu s § 16 školského zákona, a o závěrech vyšetření uvedených v doporučení školského poradenského zařízení,

(e) údaje o zdravotní způsobilosti ke vzdělávání a o zdravotních obtížích, které by mohly mít vliv na průběh vzdělávání,

~~(f)~~ datum ukončení vzdělávání ve škole,

(g) jméno a příjmení zákonného zástupce, místo trvalého pobytu nebo bydliště, pokud nemá na území České republiky místo trvalého pobytu, a adresu pro doručování písemností, telefonické spojení.

5.3 Školní matrika je Správcem vedena jak v listinné tak elektronické podobě v programu Správa

MŠ.

5.4 Rozdělení přístupových práv v programu Správa MŠ

5.5 ředitelka – plný přístup

(a) statutární zástupce ředitelky – plný přístup,

(b) učitelé mateřské školy – částečný přístup k údajům dětí ve své třídě[

Zároveň s elektronickou verzí školní matriky je paralelně vedena listinná forma školní matriky, kterou vede statutární zástupce ředitelky MŠ, která je zároveň zodpovědná za její správnost, aktuálnost a řádné vedení. Aktualizace údajů o žácích a jejich zákonných zástupcích je zástupkyně povinna provádět při každé změně, a to i v průběhu roku.

6. PROSTŘEDKY A ZPŮSOB ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

6.1 Při zpracování osobních údajů je třeba volit prostředky, které jsou přiměřené z hlediska účelu zpracování. Je nutné postupovat tak, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také je třeba dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

6.2 Ke zpracování osobních údajů je třeba souhlasu subjektu údajů, nevyplývá-li ze *Záznamu o činnostech zpracování osobních údajů (čl. 30 GDPR)*, že Správce má jiný právní důvod zpracování. V takovém případě probíhá zpracování na základě jiného právního důvodu, a to pro:

(a) splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

(b) splnění právní povinnosti, která se vztahuje na Správce;

(c) ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

(d) splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce pověřen;

(e) účely oprávněných zájmů Správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

6.3 Osobní údaje lze zpracovávat v listinné podobě a/nebo elektronicky, a to v souladu se zásadami zabezpečení uvedenými zejména v *článcích 11 až 13*.

7. PRÁVA SUBJEKTŮ ÚDAJŮ

7.1 Podle Nařízení mají subjekty údajů možnost využít svého práva požadovat po Správci

(i) přístup ke svým osobním údajům;

(ii) opravu osobních údajů;

(iii) výmaz osobních údajů;

(iv) omezení zpracování údajů týkajících se subjektu údajů;

(v) právo vznést námitku proti zpracování; a

7.2 Pokud kterákoliv osoba vázána touto Směrnicí obdrží jakoukoliv žádost související s uplatněním práva subjektů údajů, zavazuje se tato osoba dodržovat stanovené postupy pro vypořádání těchto žádostí subjektů údajů. Konkrétní postupy pro vypořádávání uplatněných práv subjektů údajů jsou popsány v této Směrnici, případně tyto postupy stanoví ředitel, resp. ředitelka organizace Správce (dále též „**Odpovědná osoba**“), který může pověřit řešením žádosti též dalšího zaměstnance, přičemž odpověď žadateli je vždy zpracována ve spolupráci s DPO, který je o žádosti vždy bezprostředně informován. Odpověď je odesílána žadateli po jejím schválení DPO.

PRÁVO NA PŘÍSTUP K OSOBNÍM ÚDAJŮM

7.3 Uplatní-li subjekt údajů právo na přístup ke svým osobním údajům dle čl. 15 Nařízení, je mu

Správce povinen tuto informaci předat bez zbytečného odkladu, anebo nejpozději do 30 dnů ode dne doručení žádosti. Informace jsou poskytnuty ve formě, ve které subjekt údajů uplatňuje své právo.

7.4 Správce je povinen před sdělením informací o zpracování v rámci uplatněného práva na přístup ze strany subjektu údajů ověřit identitu dotazujícího se subjektu údajů. K ověření identity subjektu údajů, který žádá o přístup k osobním údajům, využije Správce všech vhodných opatření. Není-li Správce schopen dostatečně identifikovat subjekt údajů, informuje ho o této skutečnosti, pokud je to možné. Ověřování identity není Správcem zneužíváno k získávání dalších údajů a k jejich uchování za jinými účely než je reakce na konkrétní žádost subjektu údajů. V případě práva subjektu údajů požadovat provedení faktického úkonu bude identita žadatele ověřena na základě jeho elektronického podpisu nebo komunikací prostřednictvím datové schránky, není li tomu tak, osobním podpisem žádosti. V případě žádosti o písemné sdělení bude identita žadatele ztotožněna doručením odpovědi do vlastních rukou žadatele s vyloučením možnosti vhození do poštovní schránky žadatele po uplynutí úložní lhůty na poště.

7.5 Obsahem informace uvedené v *článku 9.4* je sdělení o:

(i) účelu zpracování osobních údajů dle příslušné položky záznamů o zpracování osobních údajů,

(ii) osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování dle příslušné položky záznamů o zpracování osobních údajů,

(iii) příjemci, případně kategoriích příjemců dle příslušné položky záznamů o zpracování osobních údajů,

(iv) době, po kterou budou osobní údaje uloženy dle příslušné položky záznamů o zpracování osobních údajů,

(v) existenci práva požadovat od Správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování,

(vi) právu podat stížnost u ÚOOÚ,

(vii) veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů, a

(viii) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a v těchto případech smysluplné informace týkající se použitého postupu, jakož i sdělení o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů.

7.6 Informace dle *článku 9.5* je poskytována v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

ODVOLÁNÍ SOUHLASU SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

7.7 Subjekt údajů může kdykoli, i bez uvedení důvodů, odvolat souhlas se zpracováním osobních údajů.

7.8 Osobní údaje, zpracovávané na základě souhlasu subjektu údajů, budou bez zbytečného odkladu zlikvidovány, ledaže by existoval jiný právní základ pro zpracování (např. plnění smlouvy, plnění právní povinnosti), který vyžaduje uchovávání osobních údajů po minimální dobu nebo pro dosažení určitého účelu.

7.9 V rámci likvidace osobních údajů musí dojít k jejich výmazu ze všech úložišť, zejména tedy ze všech papírových a elektronických databází, webových stránek apod. Za tím účelem musí Odpovědná osoba neprodleně po obdržení žádosti subjektu údajů kontaktovat odpovědné zaměstnance a případné zpracovatele a získat jejich písemné potvrzení o likvidaci osobních údajů.

ŽÁDOST O OPRAVU OSOBNÍCH ÚDAJŮ

7.10 Subjekt údajů může kdykoli požádat o opravu nepřesných osobních údajů, které se ho týkají, nebo doplnění neúplných osobních údajů. Oprava se může týkat pouze osobních údajů, nikoli jejich hodnocení.

7.11 Osobní údaje se bezodkladně po přijetí žádosti opraví ve všech úložištích, zejména tedy ve všech papírových a elektronických databázích, webových stránkách apod. Za tím účelem musí Odpovědná osoba ve spolupráci s DPO neprodleně po obdržení žádosti subjektu údajů kontaktovat odpovědné zaměstnance a případné zpracovatele a získat jejich písemné potvrzení o opravě osobních údajů. Poté DPO informuje subjekt údajů.

ŽÁDOST O VÝMAZ / PRÁVO BÝT ZAPOMENUT

7.12 Právo na výmaz osobních údajů může subjekt údajů uplatnit v následujících případech:

(i) Osobní údaje již nejsou nezbytné pro účel, pro které byly shromažďovány a / nebo zpracovány.

(ii) Subjekt údajů odvolal souhlas se zpracováním údajů podle článku 7 Nařízení.

(iii) Subjekt údajů uplatnil právo vznést námitku podle článku 21 Nařízení.

(iv) Osobní údaje byly zpracovány protiprávně.

(v) Existuje zákonná povinnost vymazat osobní údaje.

(vi) Osobní údaje byly shromážděny od dítěte mladšího 16 let (nebo jiná věková hranice podle adaptačního zákona ke GDPR) pro poskytování služeb informační společnosti.

7.13 Po podání žádosti budou osobní údaje, které jsou předmětem výkonu práva na výmaz, bez zbytečného odkladu zlikvidovány, ledaže by existoval jiný právní základ pro zpracování (např. plnění smlouvy, plnění právní povinnosti), který vyžaduje uchovávání osobních údajů po minimální dobu nebo pro dosažení určitého účelu.

7.14 Osobní údaje budou vymazány ze všech úložišť, zejména tedy ze všech papírových a elektronických databází, webových stránek apod. Za tím účelem musí Odpovědná osoba ve spolupráci s DPO neprodleně po obdržení žádosti subjektu údajů kontaktovat kontaktovat odpovědné zaměstnance a případné zpracovatele a získat jejich písemné potvrzení o výmazu osobních údajů. Poté DPO informuje subjekt údajů.

ŽÁDOST O OMEZENÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

7.15 Žádost subjektu údajů o omezení zpracování osobních údajů, s výjimkou uchovávání, vyvolá zákaz jakéhokoli zpracování osobních údajů, které jsou předmětem žádosti, ledaže se uplatní některá z následujících výjimek:

(i) Je udělen souhlas subjektu údajů.

(ii) Zpracování osobních údajů je nezbytné pro uplatnění práva u soudu.

(iii) Zpracování osobních údajů je nezbytné pro ochranu práv jiné fyzické nebo právnické osoby.

(iv) Zpracování osobních údajů vyžaduje veřejný zájem.

7.16 Subjekt údajů má právo žádat správce o omezení zpracování osobních údajů v následujících případech:

(i) Porušení zákonnosti zpracování osobních údajů.

(ii) Podání žádosti o opravu údajů podle článku 16 Nařízení, až do té doby, než bude tato oprava provedena.

(iii) V případě podání námitek proti zpracování osobních údajů podle článku 21 Nařízení.

7.17 Za tím účelem musí Odpovědná osoba ve spoupráci s DPO neprodleně po obdržení žádosti subjektu údajů kontaktovat kontaktovat odpovědné zaměstnance a případné zpracovatele a získat jejich písemné potvrzení o omezení zpracování osobních údajů (osobní údaje jsou označeny jako s omezeným zpracováním až do dalšího rozhodnutí). Poté DPO informuje subjekt údajů. Před

zrušením omezení zpracování osobních údajů musí být subjekt údajů informován.

ŽÁDOST O UMOŽNĚNÍ PŘENOSITELNOSTI OSOBNÍCH ÚDAJŮ

7.18 Subjekt údajů má právo na poskytnutí jeho osobních údajů, které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu.

7.19 Subjekt údajů může požadovat přenositelnost svých osobních údajů pouze v případě automatizovaného zpracování a pouze pokud jsou osobní údaje:

(i) Zpracovávány se souhlasem subjektu údajů.

(ii) Zpracovávány na základě smlouvy uzavřené se subjektem údajů.

(iii) Poskytované výlučně subjektem údajů.

7.20 Za tím účelem musí Odpovědná osoba ve spolupráci s DPO neprodleně po obdržení žádosti subjektu údajů kontaktovat odpovědné zaměstnance a jejich prostřednictvím případné zpracovatele a získat od nich osobní údaje subjektu údajů v běžně používaném a strojově čitelném formátu. Poté DPO informuje subjekt údajů a předá mu příslušné osobní údaje.

NÁMITKA PROTI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

7.21 Po doručení námitky proti zpracování osobních údajů DPO ve spolupráci s Odpovědnou osobou posoudí její přiměřenost a důvodnost. Během tohoto hodnocení musí být zpracování omezeno na rozsah odpovídající účelu určení, výkonu nebo obhajoby právních nároků.

7.22 Bude-li vznesená námitka vyhodnocena jako oprávněná, Správce dále nezpracovává osobní údajů subjektu údajů a provede jejich likvidaci.

7.23 Subjekt údajů může vznést námitky proti zpracování osobních údajů v následujících případech:

(i) Zpracování je prováděno pro účely přímého marketingu včetně případného profilování; Správce nesmí námitku odmítnout.

(ii) Pokud je zpracování osobních údajů prováděno pro vědecké nebo historické účely nebo pro statistické účely; Správce může takovou námitku odmítnout, pouze pokud je zpracování osobních údajů nezbytné pro plnění úkolů veřejného zájmu.

(iii) Pokud je zpracování jeho údajů založeno na oprávněném zájmu správce údajů, včetně případného profilování; Správce může takovou námitku odmítnout, pokud:

(a) Existují legitimní důvody, které převažují nad právy subjektu údajů; nebo

(b) Zpracování osobních údajů je nezbytné pro uplatnění práva.

7.24 Za tím účelem musí Odpovědná osoba ve spolupráci s DPO neprodleně po obdržení žádosti subjektu údajů kontaktovat odpovědné zaměstnance a jejich prostřednictvím případné zpracovatele a zajistit jejich součinnost při vyřízení námitky subjektu údajů. Poté DPO informuje subjekt údajů.

ČASOVÝ RÁMEC

7.25 DPO odpoví či zajistí odeslání odpovědi na žádost subjektu údajů do jednoho měsíce od obdržení žádosti. Tuto lhůtu lze přiměřeně prodloužit, a to až na tři měsíce od obdržení žádosti, v případech zvlášť složitých, a to oznámením subjektu údajů učiněným do jednoho měsíce od obdržení žádosti.

7.26 Pokud DPO zjistí důvody pro odmítnutí žádosti, informuje subjekt údajů do jednoho měsíce od obdržení žádosti a uvede:

(i) Důvody odmítnutí žádosti.

(ii) Možnost podání stížnosti ÚOOÚ.

(iii) Možnost podání žaloby u soudu.

7.27 V případě zjevně neopodstatněných, nedůvodných nebo opakovaných žádostí může Správce

odmítnout vyhovět žádosti. V takovém případě DPO vyrozumí subjekt údajů do jednoho měsíce od obdržení žádosti.

ZPŮSOB VYŘIZOVÁNÍ ŽÁDOSTÍ

7.28 Odpověď poskytnutá subjektu údajů musí být jasná a úplná. Jazyk odpovědi musí být jasný a srozumitelný.

7.29 Odpověď na žádost subjektu údajů je poskytnuta písemně. Pokud subjekt údajů požádá o ústní odpověď, DPO na takovou žádost přiměřeně zareaguje, učiní o tom písemný záznam a navíc zašle subjektu údajů písemnou odpověď.

7.30 Při poskytování písemné odpovědi na žádost subjektu údajů použije DPO především formuláře uvedené v příloze č. 2.

NÁKLADY

7.31 Výkon práv subjektů údajů je bezplatný, s výjimkou následujících případů, kdy Správce může účtovat subjektu údajů přiměřený poplatek podle skutečných administrativních nákladů:

(i) Zjevně neopodstatněné, nedůvodné nebo opakované žádosti podle článku 12.5 Nařízení.

(ii) Žádosti o více kopií osobních údajů v případě žádosti o přístup podle článku 15.3 Nařízení.

7.32 Účtování poplatku dle předchozího bodu vždy Správce konzultuje s DPO.

EVIDENCE ŽÁDOSTÍ

7.33 DPO uchovává v elektronickém úložišti záznamy o žádostech subjektů údajů, řazené podle data podání žádosti spolu s příslušným dokladem o poskytnutí odpovědi. V elektronickém úložišti budou uchovány též další údaje týkající se posouzení a rozhodnutí o žádosti (např. důvody odmítnutí žádosti atd.).

8. ZAPOJENÍ ZPRACOVATELE A NÁLEŽITOSTI SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

8.1 Správce může zpracováním osobních údajů pověřit třetí osobu (zpracovatele). Pověření lze udělit pouze v rámci smlouvy, která splňuje náležitosti čl. 28 odst. 3 Nařízení, přičemž Správce vynaloží přiměřené úsilí, aby zpracování osobních údajů bylo založeno na vzorové smlouvě o zpracování osobních údajů v písemné formě, která je přílohou této Směrnice.

8.2 Pokud má Správce v úmyslu uzavřít smlouvu o zpracování osobních údajů, která není přílohou této Směrnice, znění smlouvy konzultuje s DPO. Správce postupuje stejně i v případě, že si zpracovatel vyžádá úpravy smlouvy o zpracování osobních údajů, která je přílohou této Směrnice.

8.3 Smlouva o zpracování osobních údajů musí zavazovat zpracovatele k dodržování této Směrnice. V této smlouvě o zpracování osobních údajů musí být výslovně stanoven předmět a doba trvání zpracování, povaha a účel zpracování, kategorie osobních údajů a kategorie subjektů údajů, práva a povinnosti Správce a záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů v rozsahu přijatelném pro Správce. Předchozí věta nevylučuje povinnost zpracovatele zajistit vyšší stupeň ochrany, a to zejména v případě, že zpracovatel bude pověřen zpracováním takových údajů, které Správce sám nezpracovává a jejichž zpracování vyžaduje vyšší bezpečnost.

8.4 Smlouva o zpracování osobních údajů stanoví zejména, že zpracovatel:

(a) zpracovává osobní údaje pouze na základě doložených pokynů Správce, včetně v otázkách případného předání osobních údajů do třetí země, pokud mu toto zpracování již neukládá právo České republiky nebo Evropské unie;

(b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

(c) přijme opatření k zabezpečení osobních údajů dle čl. 32 Nařízení;

(d) dodržuje podmínky pro zapojení dalšího zpracovatele, především nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce a dále dodržuje povinnost vyplývající z *článku 8.5*;

(e) zohledňuje povahu zpracování, je Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů;

(f) je Správci nápomocen při zajišťování souladu s povinnostmi při zabezpečení osobních údajů, ohlašování a oznamování případů porušení zabezpečení osobních údajů ÚOOÚ a subjektu údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace;

(g) v souladu s rozhodnutím Správce všechny osobní údaje buď vymaže, nebo je vrátí Správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo České republiky nebo Evropské unie nepožaduje uložení daných osobních údajů;

(h) poskytne Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověřil, a k těmto auditům přispěje.

8.5 Ze smlouvy o zpracování osobních údajů musí také vyplývat závazek zpracovatele, že nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce. V případě obecného písemného povolení musí být zpracovatel zavázán informovat Správce o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytnout tak Správci příležitost vyslovit vůči těmto změnám námitky.

8.6 Pokud zpracovatel využije ke zpracování osobních údajů třetích osob (dalších zpracovatelů), je povinen zajistit, aby dodržovaly obdobně ustanovení smlouvy o zpracování osobních údajů tak, aby nedošlo ke snížení úrovně ochrany osobních údajů zajištěné touto Směrnicí.

8.7 Pokud Správce zpracovává pro jiného správce osobní údaje v roli zpracovatele, uplatní se tato Směrnice obdobně, nestanoví-li smlouva mezi Správcem a tímto jiným správcem jinak.

8.8 Ve výjimečných případech, kdy nedochází k dlouhodobému a systematickému zpracování osobních údajů, např. pokud existuje pouze nahodilá možnost přístupu smluvní strany k osobním údajům, jejichž zpracování není primárním účelem smluvního vztahu, lze namísto smlouvy o zpracování osobních údajů uzavřít, po předchozím schválení ze strany DPO, dohodu o mlčenlivosti přiměřeně aplikující požadavky čl. 28 odst. 3 Nařízení na konkrétní jednotlivý případ.

9. POUČOVACÍ A INFORMAČNÍ POVINNOST, PRÁVO NA PŘÍSTUP K ÚDAJŮM

9.1 V případě, kdy Správce získal osobní údaje od subjektu údajů, je povinen jej poučit ve smyslu čl. 13 Nařízení. Poučení lze provést i informací o zpracování osobních údajů, zveřejněnou na webových stránkách Správce, uvedením textu poučení nebo odkazu v protokole o jednání, kterého se subjekt údajů zúčastnil, v rámci poučení v písemném vyhotovení procesního úkonu Správce nebo jiným vhodným způsobem. Správce efektivně využívá výjimky z informační povinnosti, dané čl. 13 odst. 4 Nařízení, tedy neinformuje, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má. Nelze-li postupovat žádným z výše uvedených způsobů, Správce vynaložení přiměřené úsilí, aby se subjekt údajů seznámil s textem poučení uvedeného v příloze č. 2.

9.2 V případě, že osobní údaje nebyly získány od subjektu údajů, je Správce povinen jej poučit ve smyslu čl. 14 Nařízení. Poučení lze provést i informací o zpracování osobních údajů, zveřejněnou na webových stránkách Správce, uvedením textu poučení nebo odkazu v protokole o jednání, kterého se subjekt údajů zúčastnil, v rámci poučení v písemném vyhotovení procesního úkonu Správce nebo jiným vhodným způsobem. Správce efektivně využívá výjimky z informační povinnosti, dané čl. 14 odst. 5 Nařízení, tedy tedy neinformuje, pokud

(a) subjekt údajů již uvedené informace má;

(b) se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí, nebo pokud je pravděpodobné, že uplatnění povinnosti uvedené v odstavci 1 tohoto článku by znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování;

(c) je získávání nebo zpřístupnění výslovně stanoveno právním předpisem – tuto výjimku Správce aplikuje vždy, jedná-li se o výkon činností Správce, upravený právním předpisem, zejména školským zákonem;

(d) osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právním předpisem, včetně zákonné povinnosti mlčenlivosti.

Nelze-li postupovat žádným z výše uvedených způsobů, Správce vynaložení přiměřené úsilí, aby se subjekt údajů seznámil s textem poučení uvedeného v příloze č. 2.

9.3 Informace uvedené v *článku 9.1* poskytne Správce subjektu údajů nejpozději v okamžiku získání osobních údajů a informace uvedené v *článku 9.2* poskytne Správce subjektu údajů v přiměřené lhůtě po získání osobních údajů, ale nejpozději do 30 dnů, nelze-li aplikovat příslušnou výjimku z informační povinnosti. V případech, kdy mají být osobní údaje použity pro účely komunikace, poskytne Správce tyto informace v okamžiku, kdy poprvé dojde k této komunikaci, anebo pokud mají být osobní údaje zpřístupněny jinému příjemci, poskytne Správce informace při prvním zpřístupnění osobních údajů.

9.4 Uplatní-li subjekt údajů právo na přístup ke svým osobním údajům dle čl. 15 Nařízení, je mu Správce povinen tuto informaci předat bez zbytečného odkladu, anebo nejpozději do 30 dnů ode dne doručení žádosti. Informace jsou poskytnuty ve formě, ve které subjekt údajů uplatňuje své právo.

9.5 Obsahem informace uvedené v *článku 9.4* je sdělení o:

(a) účelu zpracování osobních údajů,

(b) osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování,

(c) příjemci, případně kategoriích příjemců dle položky Předávání třetím stranám v Záznamech o činnostech zpracování osobních údajů (čl. 30 Nařízení),

(d) době, po kterou budou osobní údaje uloženy dle položky Plánovaná doba uchování osobních údajů v Záznamech o činnostech zpracování osobních údajů (čl. 30 Nařízení),

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

(f) právu podat stížnost u ÚOOÚ,

(g) veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů, a

(h) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a v těchto případech smysluplné informace týkající se použitého postupu, jakož i sdělení o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů.

9.6 Informace dle *článku 9.5* je poskytována v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

10. PŘEDÁVÁNÍ A ZÍSKÁVÁNÍ OSOBNÍCH ÚDAJŮ

10.1 Předávání osobních údajů třetím osobám je zakázáno, nestanoví-li *položky Předávání třetím stranám v Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)* jinak. Předání nebude umožněno bez souhlasu subjektu údajů, není-li takové předávání možné uskutečnit na základě zákonného důvodu i bez souhlasu subjektu údajů. Seznam kategorií příjemců je uveden *v Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)*. Při předávání osobních údajů musí Správce přijmout taková opatření, aby byla zajištěna jejich bezpečnost na úrovni požadované zejména *články 11 až 13*. Správce uzavírá za účelem předá(vá)ní osobních

údajů s příjemcem písemnou smlouvu, v níž se příjemce především zaručí za zajištění bezpečnosti předaných osobních údajů, zejména (nikoliv však výlučně) pak zastavit zpracování osobních údajů v případě, že subjekt údajů svůj souhlas odvolá a toto oznámí Správci. Povinnost podle předchozí věty se nevztahuje na předání nebo zpřístupnění příslušným státním orgánům a dalším osobám, jež upravují zvláštní právní předpisy (např. soudy, Policie ČR, orgány péče o dítě, lékařská služba, atd.).

10.2 Získávání osobních údajů od jiných správců je možné pouze na základě písemné smlouvy. Podmínky tohoto smluvního vztahu musí odpovídat zejména zárukám ve vztahu k oprávněnosti předchozího zpracování osobních údajů a zejména (nikoliv však výlučně) zárukám, že subjekty údajů poskytly souhlas s předáním jejich osobních údajů dalším správcům, aniž by vyloučily Správce. Uzavření takové smlouvy Správce vždy konzultuje s DPO.

10.3 *Článek 10.2* se nepoužije v případě, že osobní údaje subjektů údajů nebo třetích osob jsou získávány v souvislosti s plněním smlouvy se subjekty údajů či na základě jiného právního důvodu, pro který je možné zpracovávat osobní údaje bez souhlasu subjektu údajů; konkrétně se jedná o důvody uvedené v čl. 6 odst. 1 písm. b) až f) Nařízení, příp. čl. 9 odst. 1 písm. b) až j) jedná-li se o zvláštní kategorii osobních údajů. V tomto případě, stejně jako v předchozím případě dle předchozího *článku 10.2*, je Správce povinen zajistit poučení a informaci podle *článku 9.2* před dalším zpracováním, ledaže lze aplikovat výjimky tam uvedené.

11. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ: OPRÁVNĚNÉ OSOBY A ROZSAH OPRÁVNĚNÍ

11.1 Ředitel, resp. ředitelka Správce určí osoby oprávněné pro nakládání s osobními údaji v rozsahu nezbytném pro výkon příslušné agendy.

11.2 Osobám nakládajícím v rámci své agendy s osobními údaji zajistí Správce ve spolupráci s DPO proškolení ohledně správného nakládání s osobními údaji, a to před tím, než je jim nakládání s osobními údaji umožněno. Za poskytnutí řádného školení odpovídá ředitel, resp. ředitelka Správce ve spolupráci s DPO; tak, aby tyto osoby absolvovaly příslušné školení alespoň jednou ročně.

11.3 Osoby oprávněné k nakládání s osobními údaji schvaluje a případně upravuje Odpovědná osoba, přičemž tato pravidelně aktualizuje *položky Kdo má k osobním údajům přístup v Záznamu o činnostech zpracování osobních údajů (čl. 30 GDPR)* postupem dle *článku 15*.

11.4 Nikdo nesmí nakládat s osobními údaji nad rámec svého oprávnění, jak je vymezeno v konkrétní pracovní pozice v *Záznamu o činnostech zpracování osobních údajů (čl. 30 GDPR)*. Osoby neuvedené na Seznamu nesmí osobní údaje zpracovávat ani k nim přistupovat.

11.5 Individuální výjimky ze zákazu podle *článku 11.4* může výslovně udělit Odpovědná osoba. V takovém případě je povinna specifikovat pro jaký úkon a na jakou dobu se výjimka uděluje; vždy by se mělo jednat o postup výjimečný, odůvodněný objektivními důvody a vyžaduje-li to povaha zpracování, např. z důvodu citlivé povahy kategorií zpracovávaných osobních údajů anebo většího rozsahu údajů, měla by být výjimka ze zákazu písemná. Udělení výjimky konzultuje Odpovědná osoba s DPO.

12. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ: TECHNICKÉ ZABEZPEČENÍ PÍSEMNOSTÍ A JINÝCH FYZICKÝCH NOSIČŮ

12.1 Veškeré písemnosti a jiné fyzické nosiče informací, kterými Správce disponuje a které obsahují osobní údaje chráněné Nařízením či Zákonem, musí být chráněny před volným přístupem neoprávněných osob, především skladováním v uzamykatelných skříňkách, které jsou umístěny v uzamykatelných místnostech chráněných proti požáru.

12.2 Správce vede evidenci přístupu do jednotlivých uzamykatelných místností, například ve formě evidence vydaných klíčů. Obdobným způsobem Správce eviduje přístupnost uzamykatelných skříněk, které obsahuje písemnosti nebo jiné fyzické nosiče informací, které obsahují osobní údaje.

12.3 Bezprostřední přístup k těmto materiálům mají pouze osoby uvedené na Seznamu, a to pouze v rozsahu tam uvedeného oprávnění či v rozsahu individuální výjimky udělené v souladu s *článkem 11.5*.

13. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ: TECHNICKÉ ZABEZPEČENÍ ELEKTRONICKÝCH DAT

13.1 Osobní údaje obsažené v elektronické formě na datovém nosiči informací musí být uloženy buď na samostatných datových nosičích umístěných v uzamykatelných skříních, a/nebo místnostech přístupných pouze osobám uvedeným v Seznamu anebo na serveru, k němuž mají fyzický přístup pouze osoby k tomu oprávněné dle Seznamu. Tento server (a další prvky ICT infrastruktury, jako jsou přepínače, směrovače atd.), musí být umístěn v uzamykatelné místnosti s režimovým přístupem.

13.2 Počítač nebo notebook, na kterém jsou data obsahující osobní údaje uložena, musí být chráněn proti útoku z internetu antivirovým systémem či obdobnými zabezpečovacími prostředky, které musí být odpovídajícím způsobem monitorovány a aktualizovány. Datové soubory musí být šifrovány, pokud je to možné.

13.3 K přístupu k datovým souborům jsou oprávněny pouze osoby na základě jejich systemizovaného pracovního místa, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, a to v rozsahu potřebném pro výkon jejich činnosti.

13.4 Systém musí pořizovat elektronické záznamy, které umožní určit a ověřit, kdy a kým byly osobní údaje zaznamenány nebo jinak zpracovány

13.5 Datové soubory obsahující osobní údaje, jejichž ztráta nebo změna by mohla mít negativní důsledky pro subjekty údajů, musejí být pravidelně, alespoň jednou za dva týdny, zálohovány.

13.6 Za účelem zajištění ochrany ve smyslu *článků 13.2 až 13.5* musí informační systém nebo jeho implementace zajišťovat alespoň tyto bezpečnostní funkce:

(a) zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením.; -

(b) možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele, bezpečnostního správce nebo správce informačního systému;

(c) možnost pseudonymizace a šifrování osobních údajů

(d) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.

13.7 Za elektronickou ochranu osobních údajů odpovídá systémový administrátor, jehož pověřuje Správce („**Systémový administrátor**“), buď na základě smluvního dodavatelského vztahu či zajištěním této funkce zaměstnancem organizace prostřednictvím jeho pracovní náplně. Není li systémový administrátor určen, za plnění jeho povinností odpovídá ředitel, resp. ředitelka Správce.

13.8 V případě opravy informačního systému zajistí Systémový administrátor, že osoby, které budou tuto opravu provádět, jsou důvěryhodné a budou vázány povinností mlčenlivosti ve smyslu *článku 14*, a to pod hrozbou smluvní pokuty.

14. POVINNOST MLČENLIVOSTI

14.1 Všechny osoby, které zpracovávají osobní údaje pro Správce, jakož i další osoby, které přijdou do styku s osobními údaji u Správce nebo zpracovatele, jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních přijatých podle této Směrnice. Povinnost mlčenlivosti trvá i po skončení příslušných prací.

14.2 Výjimky z povinnosti mlčenlivosti se řídí platnými a účinnými právními předpisy. Vždy nicméně platí, že pokud osobě vázané touto Směrnicí vznikne podle příslušných právních předpisů informační povinnost, která je vyňata z povinnosti mlčenlivosti, uvědomí o tom tato osoba neprodleně ředitele, ředitelku Správce a zajistí, že osoba, jíž bude informace v rámci výjimky z povinnosti mlčenlivosti sdělena, si bude vědoma jejího důvěrného charakteru.

15. ZAJIŠTĚNÍ AKTUÁLNOSTI ÚDAJŮ A OPRÁVNĚNÝCH OSOB

15.1 Odpovědná osoba vede Seznam oprávněných osob podle *článku 11.1* a odpovídá za jeho pravidelnou aktualizaci, přičemž aktuální seznam je k dispozici DPO. K aktualizaci musí dojít pokaždé, kdy dojde ke změně v okruhu oprávněných osob či rozsahu jejich oprávnění. Zvláště to platí v případech, kdy dosavadní zaměstnanec Správce přestal být u Správce zaměstnán. Osoba odpovědna za vedení Seznamu je povinna zajistit reflexi těchto změn při nastavení zabezpečení písemností a jiných fyzických nosičů osobních údajů dle *článku 12*.

15.2 Osoby vázané touto Směrnicí jsou povinny hlásit DPO veškeré změny týkající se oprávněných osob a rozsahu jejich oprávnění.

15.3 Odpovědná osoba informuje Systémového administrátora o změnách v Seznamu oprávněných osob a rozsahu jejich oprávnění. Systémový administrátor je povinen zajistit reflexi těchto změn při nastavení obsahu a zabezpečení elektronických datových souborů dle *článku 13*.

16. LIKVIDACE

16.1 Správce nebo na základě jeho pokynu zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány; postupuje se zejména podle harmonogramu stanoveného v *položce Plánovaná doba uchování osobních údajů v Záznamu o činnostech zpracování osobních údajů (čl. 30 GDPR)* a Skartačního řádu.

16.2 Likvidaci je třeba provést také v případě, kdy subjekt údajů požádá o ukončení zpracování osobních údajů nebo vezme zpět svůj souhlas se zpracováním osobních údajů, je-li tento nezbytný pro další zpracování, nesvědčí-li Správci jiný právní titul pro zpracování osobních údajů.

16.3 Správce ve spolupráci s DPO zajistí koordinaci likvidace osobních údajů se zpracovateli a příjemci osobních údajů.

16.4 Obvyklým způsobem likvidace je

(a) skartování či jiné zničení neumožňující zpětnou rekonstrukci písemných dokumentů,

(b) anonymizace identifikačních údajů v počítačových databázích (za předpokladu, že s tímto subjekt údajů vyslovil souhlas), nebo

(c) jejich vymazání, a to bez možnosti jejich opětovného obnovení (pomocí příslušných softwarových nástrojů).

16.5 O likvidaci se provede zápis, který bude uložen u DPO; tento zápis bude obsahovat identifikaci příslušné databáze a kategorie zlikvidovaných osobních údajů a dále důvod, pro který byla likvidace provedena.

17. POVINNOST VYPRACOVAT DOKUMENT POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ A POVINNOST PŘEDCHOZÍ KONZULTACE S ÚOOÚ

17.1 Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede Správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů („**Posouzení**“ nebo „**DPIA**“). Pro soubor podobných operací zpracování, které představují podobné riziko, může být zpracováno pouze jedno Posouzení.

17.2 Při provádění DPIA si Správce vyžádá posudek DPO.

17.3 Posouzení vlivu na ochranu osobních údajů podle *článku 17.1* Správce povinně vypracovává

v případech, pokud se v rámci zpracování jedná o:

(a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

(b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 Nařízení nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10 Nařízení;

(c) rozsáhlé systematické monitorování veřejně přístupných prostorů; nebo

(d) zpracování, které podléhá požadavku na posouzení vlivu na ochranu osobních údajů dle seznamu sestaveného ÚOOÚ (pozitivní seznam).

17.4 Správce není povinen DPIA vyhotovovat v případech, kdy daná činnost zpracování spadá pod činnosti dle seznamu druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné, sestaveného ÚOOÚ (negativní seznam).

17.5 Posouzení má formu dokumentu, který obsahuje alespoň:

(a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů Správce;

(b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

(c) posouzení rizik pro práva a svobody subjektů údajů uvedených v *článku 17.1*; a

(d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s Nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

17.6 Správce případně provede přezkum s cílem posoudit, zda je zpracování prováděno v souladu s provedeným DPIA alespoň v případech, kdy dojde ke změně rizika, jež představují operace zpracování.

18. KONTINGENČNÍ PLÁN A OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

18.1 Jakékoliv porušení zabezpečení osobních údajů („**Porušení**“), zejména ztrátu, odcizení, poškození či zničení osobních údajů je každá osoba, která se o takové skutečnosti dozví, povinna neprodleně oznámit svému řediteli, resp. ředitelce Správce a současně i DPO.

A) OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ ÚOOÚ

18.2 DPO ohlásí v souladu s *článkem 18.1* případ Porušení ÚOOÚ bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy mu bylo toto Porušení ohlášeno, ledaže je nepravděpodobné, že by toto Porušení mělo za následek riziko pro práva a svobody fyzických osob.[2]

18.3 Ohlášení podle *článku 18.2* obsahuje zejména tyto informace:

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

(b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

[2] Příkladem porušení, které nevyžaduje ohlášení, je ztráta bezpečně zašifrovaného mobilního zařízení používaného správcem a jeho zaměstnanci. Za podmínky, že šifrovací klíč zůstal v bezpečném držení správce a nejde o jedinou kopii osobních údajů, jsou osobní údaje pro útočníka v zásadě nedostupné. Znamená to, že případ porušení pravděpodobně nevyústí v riziko pro práva a svobody dotčených subjektů údajů.

(c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

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

18.4 Osoba plnící ohlašovací povinnost ověří na webových stránkách ÚOOÚ (www.uoou.cz) dostupnost případného vzorového formuláře k plnění povinnosti dle *článku 18.3 (a) až (d)* a je-li formulář dostupný, vyplní údaje v požadovaném (předepsaném) rozsahu.

18.5 O dalších opatřeních v souvislosti s porušením bezpečnosti dle *článku 18.1* rozhodne DPO bez zbytečného odkladu poté, co se dozvěděl o skutečnostech uvedených v *článku 18.1*.

B) OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ SUBJEKTU ÚDAJŮ

18.6 DPO oznámí případ Porušení v souladu s *článkem 18.1* subjektům údajů, pokud je pravděpodobné, že porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

18.7 Oznámení dle *článku 18.6* je subjektu údajů poskytováno za použití jasných a jednoduchých jazykových prostředků[3] a obsahuje zejména tyto informace:

(a) popis povahy porušení zabezpečení osobních údajů;

(b) jméno a kontaktní údaje kontaktního místa Správce, které může poskytnout bližší informace;

(c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

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

18.8 Oznamovací povinnost dle *článku 18.6* není Správce povinen plnit v případě, že:

(a) Správce zajistí, že zasažené údaje jsou nesrozumitelné pro kohokoli, kdo není oprávněn k nim mít přístup (např. v případě, kdy zasažené údaje jsou nečitelné nebo nejsou přiřaditelné konkrétním osobám, např. fyzické osoby nejsou identifikovatelné díky provedení pseudonymizace nebo osobní údaje nejsou srozumitelné díky použitému šifrování apod.);

(b) Správce přijal následná opatření, která zajistí, že vysoké riziko se již pravděpodobně neprojeví (např. osobní údaje nejsou v držení třetí osoby); a/nebo

(c) by oznámení vyžadovalo nepřiměřené úsilí; v takovém případě Správce informuje subjekty údajů pomocí veřejného oznámení nebo podobného opatření.

19. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

19.1 Předávání osobních údajů do zahraničí je možno pouze v případě, jsou-li splněny podmínky stanovené Nařízením a Zákonem a je-li tak stanoveno v *položce Předávání do zahraničí v Záznamech o činnostech zpracování osobních údajů (čl. 30 GDPR)*.

19.2 DPO ve spolupráci s ředitelem, resp. ředitelkou Správce odpovídá za to, že podmínky stanovené Zákonem či Nařízením jsou splněny. Bez souhlasu DPO a oprávněné osoby Správce nelze osobní údaje do zahraničí předat.

20. SOUČINNOST

20.1 V případě, že bude nutné za účelem zajištění souladu s GDPR upravit některé stávající procesy či v současnosti prováděné operace a činnosti zahrnující shromažďování a zpracovávání osobních údajů nebo za účelem vypracování posouzení vlivu na ochranu osobních údajů, jsou osoby, na které se vztahuje tato Směrnice povinny poskytnout nezbytnou součinnost a spolupracovat s DPO

[3] Příklady způsobu transparentní komunikace zahrnují přímé textování (např. e-mail, SMS, přímá zpráva), výrazné bannery nebo oznámení na webových stránkách, komunikace poštou a nápadné reklamy v tištěných médiích.

a ředitelem, resp. ředitelkou Správce na těchto úpravách.

21. PŘECHODNÁ USTANOVENÍ

21.1 Dosud prováděné operace a činnosti obsahující shromažďování a zpracovávání osobních údajů používané do účinnosti této Směrnice musí být upraveny tak, aby byly v souladu s touto Směrnicí.

22. ÚČINNOST

Tato Směrnice nabývá platnosti a účinnosti dnem jejího vydání.

Přílohy:

1. Záznamy o činnostech zpracování osobních údajů (čl. 30 GDPR) Správce.
2. Poučení subjektů o zpracování osobních údajů a vzorové formuláře pro komunikaci se subjekty údajů.
3. Vzorová smlouva o zpracování osobních údajů.