Albrechtova střední škola,
Český Těšín, příspěvková organizace
Tyršova 611/2, 737 01 Český Těšín, IČ: 00577235
tel. 558 425 200, email: skola@albrechtovastredni.cz

SMĚRNICE

O ochraně osobních údajů

a jejich nakládání s nimi dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27 dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údaj§ a o zrušení směrnice 95/46/ES (obecného nařízení o ochraně osobních údajů)

AKTUALIZOVÁNO 1. 9. 2019

MGR. PAVEL CIESLAR

ředitel školy

Datum účinnosti 25. 5.2018

Článek 1
Účel a rozsah působnosti

1.1 Tato směrnice stanovuje práva a povinnosti při zpracování a ochraně osobních údajů, a upravuje procesní organizační opatření k zajištění povinností vyplývajících z legislativního rámce pro ochranu osobních údajů.

1.2 Směrnice se vydává v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

1.3 Směrnice upravuje povinnosti Organizace a jejích zaměstnanců při provádění automatizovaného zpracování osobních údajů a při provádění neautomatizovaného zpracování těch osobních údajů, které jsou Organizací zpracovávány. Směrnice se nevztahuje na nahodilé, neúmyslné získání osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

1.4 Organizace je v postavení Správce osobních údajů a z tohoto důvodu je zodpovědná za zpracování získávaných údajů v souladu s platnou legislativou. Organizace se zavazuje shromažďovat a vést pouze takové osobní údaje o subjektech, které umožňují poskytovat bezpečné, odborné a kvalitní služby. Pro práci s těmito osobními údaji byl vytvořen příslušný systém práce pro všechny personální úrovně, byl definován soubor osobních údajů, jejichž získávání je pro zajištění poskytování kvalitních, odborných a bezpečných služeb žákům nezbytné, dále bylo přesně vymezeno, k jakému účelu budou konkrétní osobní údaje využívány a také byla posouzena možná rizika spojená se zajištěním bezpečnosti osobních údajů a jejich správou.

1.5 Tato směrnice je závazná pro všechny zaměstnance, kteří přichází do styku s osobními údaji.

Článek 2
Použité zkratky a zástupná označení

Zkratka	Popis
DPIA	Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)
IP adresa	Jednoznačná identifikace zařízení v počítačové síti
Pověřenec	Pověřenec pro ochranu osobních údajů
Legislativní rámec	Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Zákon č. 89/2012 Občanský zákoník, Zákon o zpracování osobních údajů, kterým bude zrušen, resp. nahrazen Zákon č. 101/2000 Sb. (dle návrhu 55/2018 Sb.)
Nařízení	Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Odpovědná osoba	Osoba odpovědná za agendu zpracování osobních údajů
IT	Osoba odpovědná za zajištění informační bezpečnosti (it manager)
OÚ	Osobní údaje

Údržba	Osoba odpovědná za zajištění fyzické bezpečnosti
Organizace	Albrechtova střední škola, Český Těšín, p. o.
ZOÚ	Zaměstnanec odpovědný za ochranu osobních údajů v Organizaci (ředitel)
ICT	Informační a komunikační technologie

Článek 3
Výklad pojmů

3.1 **Osobní údaje** - veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen "subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Konkrétní osobu lze identifikovat zejména různou kombinací osobních údajů.

3.2 **Zvláštní kategorie osobních údajů** – představují ji osobní údaje, které vypovídají o národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách a hnutích, nebo odborových či zaměstnaneckých organizacích, náboženství a filosofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů.

3.3 **Subjekt údajů** - fyzická osoba, kterou lze přímo či nepřímo identifikovat pomocí osobních údajů.

3.4 **Správce** - právnická osoba, která určuje účely a prostředky zpracování osobních údajů.

3.5 **Zpracovatel** – fyzická (OSVČ) nebo právnická osoba, která zpracovává osobní údaje pro Správce.

3.6 **Likvidace osobních údajů** - je fyzické zničení nosiče osobních údajů, jejich fyzické vymazání nebo trvalé vyloučení z dalšího zpracování.

3.7 **Zpracování** - jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

3.8 **Profilování** - 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 jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

3.9 **Porušení zabezpečení osobních údajů** - porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

3.10 **Dozorový úřad** - Úřad pro ochranu osobních údajů.

3.11 **Dokument** - fyzický (papírový) dokument, nebo el. datový soubor obsahující osobní údaje

3.12 **Kopie dokumentu** – scan, fotokopie (apod.) fyzického dokumentu, anebo datová kopie el. souboru

3.13 **Zabezpečené úložiště** - datový prostor jako je centrální diskové pole, pevný disk počítačů, spisový uzel, spisovna.

3.14 **Evidence úložišť OÚ** - evidence všech úložišť, kde je možné ukládat OÚ, např.:

a) centrální datové úložiště a informační systémy
b) pevný disk osobního počítače
c) přenosné úložiště (flash disk, externí pevný disk)
d) úložiště přenosných zařízení (notebook, tablet, telefon)
e) úložiště fyzických dokumentů (spisové uzly, spisovny)

3.15 **Záznamy o činnostech zpracování** - obsahují informace o jednotlivých zpracování OÚ v Organizaci.

3.16 **Evidence porušení zabezpečení OÚ** – obsahuje dokumentaci veškerých případů porušení zabezpečení osobních údajů, přičemž jsou uvedeny skutečnosti, které se týkají daných porušení, jejich účinky a přijatá nápravná opatření.

3.17 **Evidence požadavků subjektů údajů** - obsahuje záznamy o požadavcích subjektů údajů na přístup k OÚ, opravu OÚ, výmaz OÚ, omezení zpracování a vznesení námitky včetně informace o tom, jak byly tyto požadavky vypořádány.

Část I.
Vybrané obecné podmínky pro zpracování OÚ

Článek 4
Zásady zpracování osobních údajů

4.1 OÚ musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“),

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný („účelové omezení“),

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“),

d) přesné a v případě potřeby aktualizované; 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 („přesnost“),

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány („omezené uložení“),

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“)

Článek 5
Zákonnost zpracování

5.1 Zpracování OÚ je zákonné, pokud je splněna alespoň jedna z těchto podmínek:

a) subjekt údajů udělil souhlas se zpracováním svých OÚ pro jeden či více konkrétních účelů *(čl. 6, odst. 1. a) Nařízení)*,

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů *(čl. 6, odst. 1. b) Nařízení)*,

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje *(čl. 6, odst. 1. c) Nařízení)*,

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby *(čl. 6, odst. 1. d) Nařízení)*,

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce *(čl. 6, odst. 1. e) Nařízení)*,

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného 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 *(čl. 6, odst. 1. f) Nařízení)*.

5.2 Zakazuje se zpracování zvláštní kategorie OÚ, pokud nejde o jeden z níže uvedených případů:

a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů *(čl. 9, odst. 2. a) Nařízení)*,

b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany *(čl. 9, odst. 2. b) Nařízení)*,

c) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů *(čl. 9, odst. 2. e) Nařízení)*,

d) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického významu nebo pro statistické účely, které je přiměřené sledovanému cíli, dodržuje podstatu práva na OÚ a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů *(čl. 9, odst. 2. j) Nařízení)*.

Článek 6
Souhlas se zpracováním osobních údajů

6.1 Souhlas musí být svobodným, konkrétním (pro konkrétní účel zpracování), informovaným a jednoznačným projevem vůle subjektu údajů, který jím dává své svolení ke zpracování svých osobních údajů.

6.2 Subjekt údajů musí být před udělením souhlasu informován o všech skutečnostech zpracování, zejména o Organizaci jako správci, účelech zpracování, o operacích zpracování a o možnosti kdykoli odvolat souhlas, nikoli však se zpětnými účinky.

6.3 Souhlas musí být udělen v písemné formě, a to buď v listinné, nebo v elektronické podobě.

6.4 Pokud je od Subjektu údajů nutné získat Souhlas se zpracováním, musí se tak stát za pomoci samostatného dokumentu (v listinné, nebo elektronické podobě).

6.5 Subjekt údajů je oprávněn jím udělený souhlas kdykoli odvolat. Odvolat souhlas musí být stejně snadné jako jej poskytnout. V případě, že Organizaci bude doručeno odvolání souhlasu je Organizace povinna postupovat v souladu s postupy uvedenými v této směrnici.

6.6 V případě, že subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování, Organizace je povinna provést likvidaci osobních údajů, které se daného subjektu údajů týkají.

6.7 Organizace eviduje informace o uděleném souhlasu v evidenci souhlasů se zpracováním osobních údajů

6.8 Udělený souhlas je platný pouze pro operace zpracování, které jsou nezbytné a přiměřené k naplnění účelu, pro který byl souhlas udělen.

6.9 Souhlas se zpracováním osobních údajů dítěte mladšího 15 let je platný pouze v případě, že je vyjádřen nebo schválen jeho zákonným zástupcem.

Článek 7
Zpracování zvláštních osobních údajů

7.1 Organizace smí zpracovávat zvláštní osobní údaje pouze v případech, kdy jde o některý z případů vymezených ve čl. 9 odst. 2 Nařízení, zejména

a) subjekt údajů udělil výslovný souhlas se zpracováním zvláštních osobních údajů pro jeden či více konkrétních účelů, nebo

b) zpracování je nezbytné pro účely plnění povinností vyplývajících ze smlouvy mezi subjektem a Organizací.

Článek 8
Oprávněný zájem Organizace

8.1 Organizace je oprávněna zpracovávat osobní údaje subjektu údajů v případě, je-li zpracování nezbytné pro účely plnění oprávněných zájmů Organizace či třetí osoby.

8.2 Oprávněným zájem Organizace může být např. zveřejňování osobních údajů v rámci práva na informace, ochrana před zneužitím služeb, ochrana majetkových zájmů, zajištění bezpečnosti sítě a informací a z dalších důvodů.

8.3 V každém jednotlivém případě, kdy má dojít ke zpracování osobních údajů na základě oprávněného zájmu, je nutné stanovit oprávněný zájem a dále posoudit:

a) oprávněnost stanoveného zájmu, tedy zda je stanovený zájem legální a dostatečně specifický a zda jde o skutečný zájem Organizace,

b) nezbytnost zamýšleného zpracování osobních údajů pro účely stanoveného zájmu, zda je v rovnováze oprávněný zájem Organizace a práva subjektu údajů

c) zda nad stanoveným zájmem Organizace nepřevažují zájmy nebo základní práva a svobody subjektu údajů, včetně posouzení případného přijetí záruk k ochraně práv a svobod subjektů údajů.

8.4 V případě, že jsou splněny všechny výše uvedené požadavky, smí být v rámci Organizace zahájeno zpracování osobních údajů z důvodu oprávněného zájmu.

Článek 9
Záznamy o činnostech zpracování

9.1 Každý správce vede Záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace:

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu OÚ,

b) účely zpracování,

c) popis kategorií subjektů údajů a kategorií osobních údajů,

d) kategorie příjemců OÚ, kterým byli nebo budou OÚ zpřístupněny,

e) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,

f) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

Článek 10
Posouzení vlivu na ochranu osobních údajů (DPIA)

10.1 Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním DPIA.

10.2 DPIA je nutné zejména v těchto případech:

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 OÚ nebo OÚ týkajících se rozsudků v trestních věcech a trestných činů,

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Článek 11
Zabezpečení zpracování

11.1 S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování OÚ,

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,

c) schopnosti obnovit dostupnost OÚ a přístup k nim včas v případě fyzických či technických incidentů,

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

11.2 Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných OÚ, nebo neoprávněný přístup k nim.

11.3 Zpracovat a evidovat přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů v souladu s Nařízením a zvláštními a interními předpisy.

11.4 Zajistit, že užívat systémy pro automatizované zpracování osobních údajů mohou pouze oprávněné osoby, a to pouze v rozsahu odpovídajícímu jejich oprávnění,

11.5 Zajistit elektronické záznamy o přístupu k osobním údajům a provedených úkonech i zpracování osobních údajů.

11.6 Zabránit neoprávněnému přístupu k nosičům informací.

11.7 Posoudit, zda bude docházet k předání osobních údajů třetím osobám a zda jsou splněny všechny podmínky předání v souladu s Nařízením a touto směrnicí.

Článek 12
Uzavírání smluv se zpracovateli OÚ

12.1 Pro zpracování OÚ využije Správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení a aby byla zajištěna dostatečná ochrana práv subjektu údajů.

12.2 Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího písemného povolení Správce.

12.3 Zpracování zpracovatelem se řídí smlouvou, která zavazuje Zpracovatele vůči Správci a v níž je stanoven předmět a doba trvání, povaha a účel zpracování, typ OÚ a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt stanoví zejména, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce,

b) zajišťuje, aby se osoby oprávněné zpracovávat OÚ zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,

c) zajistí zabezpečení zpracování zejména:
- pseudonymizace a šifrování OÚ,
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
- schopnost obnovit dostupnost údajů a přístup k nim v případě fyzických či technických incidentů,
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených opatření.

d) je nápomocen při zajištění souladu s následujícími povinnostmi:
- zabezpečení zpracování,
- ohlašování případů porušení zabezpečení OÚ dozorovému úřadu,
- oznamování případů porušení zabezpečení OÚ subjektu údajů,
- posouzení vlivu na ochranu OÚ,
- předchozí konzultace (před zpracováním s dozorovým úřadem),
- v souladu s rozhodnutím správce všechny OÚ buď vymaže, anebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním a vymaže existující kopie, pokud legislativa nepožaduje uložení daných OÚ,
- poskytne správci veškeré informace potřebné k doložení toho, že byly splněny všechny povinnosti a umožní audity včetně inspekcí prováděné správcem nebo jiným auditorem, kterého správce pověřil.

Článek 13
Právo subjektu údajů na přístup k OÚ

13.1 Subjekt údajů má právo získat od správce potvrzení, zda OÚ, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto OÚ a k následujícím informacím:

a) účely zpracování,

b) kategorie dotčených OÚ,

c) příjemci nebo kategorie příjemců, kterým byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích,

d) plánovaná doba, po kterou budou OÚ uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,

e) existence práva požadovat od správce opravu nebo výmaz OÚ týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování,

f) právo podat stížnost u dozorového úřadu,

g) veškeré dostupné informace o zdroji OÚ, pokud nejsou získány od subjektu údajů,

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a informace týkající se použitého postupu.

13.2 Správce poskytne kopii zpracovávaných OÚ zdarma. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

13.3 Právem získat kopii nesmí být dotčena práva a svobody jiných osob.

Článek 14
Právo subjektu na opravu

14.1 Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné OÚ, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných OÚ, a to i poskytnutím dodatečného prohlášení.

Článek 15
Právo subjektu na výmaz („právo být zapomenut“)

15.1 Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal OÚ, které se daného subjektu údajů týkají, a správce má povinnost OÚ bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) OÚ již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování,

c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování, nebo subjekt údajů vznese námitky proti zpracování v případech zpracování pro účely přímého marketingu,

d) OÚ byly zpracovány protiprávně,

Článek 16
Právo subjektu na omezení zpracování

16.1 Subjekt údajů má právo na to, aby správce omezil zpracování v kterémkoli z těchto případů:

a) subjekt údajů popírá přesnost OÚ, a to na dobu potřebnou k tomu, aby správce mohl přesnost OÚ ověřit,

b) zpracování je protiprávní a subjekt údajů odmítá výmaz OÚ a žádá místo toho o omezení jejich použití,

c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,

d) subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Článek 17
Právo na přenositelnost údajů

17.1 Subjekt údajů má právo získat OÚ, které se ho týkají, jež poskytl Správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a právo předat tyto údaje jinému Správci, a to v případě že:

a) zpracování je založeno na souhlasu se zpracováním osobních údajů *(čl. 6, odst. 1. a) Nařízení)* nebo na souhlasu se zpracováním zvláštní kategorie osobních údajů *(čl. 9, odst. 2 a) Nařízení)* nebo na smlouvě *(čl. 6, odst. 1. a) Nařízení)*,

b) zpracování se provádí automatizovaně.

17.2 Subjekt údajů má právo na to, aby OÚ byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

17.3 Tímto právem nesmí být nepříznivě dotčena práva a svobody jiných osob.

Článek 18

Právo na podání námitky

18.1 Subjekt údajů má právo kdykoliv vnést námitku proti zpracování osobních údajů.

Článek 19
Ohlašování případů porušení zabezpečení OÚ

19.1 Jakékoli porušení zabezpečení OÚ Správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

19.2 Správce dokumentuje veškeré případy porušení zabezpečení OÚ, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí být na vyžádání přístupná dozorovému úřadu.

19.3 Pokud je pravděpodobné, že určitý případ porušení zabezpečení OÚ bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Správce toto porušení bez zbytečného odkladu subjektu údajů.

19.4 Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) Správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u OÚ dotčených porušením zabezpečení OÚ, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup, jako je např. šifrování,

b) Správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů se již pravděpodobně neprojeví,

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Část II.
Aplikace podmínek pro zpracování OÚ v Organizaci

Článek 20 Vymezení odpovědnosti

20.1 Za zpracování osobních údajů, které organizace provádí, odpovídá vždy ZOÚ. ZOÚ zodpovídá za to, že zpracování osobních údajů je prováděno v souladu s platnými právními předpisy.

20.2 ZOÚ organizace může pro oblast ochrany osobních údajů jmenovat odpovědné osoby z řad pracovníků organizace, které budou také zodpovídat za ochranu osobních údajů, a to v rozsahu, který určí ZOÚ; odpovědnost ZOÚ za zpracování osobních údajů dle této směrnice tím není nijak dotčena.

20.3 Organizace je povinna dle č. 37 a násl. jmenovat pověřence. Pověřenec vykonává svou funkci v souladu s příslušnými ustanoveními GDPR.

20.4 Moravskoslezský kraj jako zřizovatel organizace poskytuje metodickou pomoc v oblasti ochrany osobních údajů.

Článek 21 Pověřenec pro ochranu osobních údajů

21.1 Pověřenec je klíčová osoba v oblasti ochrany osobních údajů a GDPR pro rozvoj kultury ochrany osobních údajů uvnitř Organizace. Pověřenec je zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů v Organizaci a pomáhá zavádět klíčová organizační a technická bezpečnostní opatření.

21.2 Základní a neopominutelné úkoly pověřence jsou:

a) Komunikovat se subjekty údajů, které mají právo se na něj obracet dle Čl. 38, odst. 4 Nařízení. Pověřenec například poskytuje informace o zpracování nebo o právech subjektu údajů podle Nařízení a jiných příslušných předpisů. Subjekty údajů jsou i zaměstnanci správce, kteří se z tohoto důvodu také mohou na pověřence obracet bez omezení.

b) Poradenství správci a zaměstnancům ohledně povinností při ochraně osobních údajů podle Čl. 39 odst. 1 písm. a) Nařízení a ohledně posouzení vlivu na ochranu osobních údajů dle Čl. 39 odst. 1 písm. c) Nařízení.

c) Zajišťuje stanoviska v průběhu tvorby posouzení vlivu.

d) Vypracovává posudek na dokončené posouzení vlivu.

e) Monitoruje soulad s předpisy na ochranu osobních údajů a s vnitřními dokumenty správce
Shromažďuje informace pro určení činností zpracování;
Analyzuje a kontroluje soulad činností zpracování;
Informuje správce nebo zpracovatele, poskytuje mu poradenství a vydávat doporučení.

f) Vyřizuje stížnosti a podněty zaměstnanců správce i dalších subjektu údajů ohledně ochrany osobních údajů.

g) Řeší incidenty týkající se ochrany osobních údajů v rámci organizace.

h) Spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro dozorový úřad. Je sice vázán mlčenlivostí, ale ta nebrání tomu, aby s dozorovým úřadem spolupracoval a konzultoval záležitosti týkající se zpracování i jakoukoli jinou otázku.

i) Své úkoly plní s přihlédnutím k riziku a povaze, rozsahu, kontextu a účelu zpracování

j) Vypracovává a předkládá vedoucímu vedení organizace pravidelné zprávy o stavu ochrany osobních údajů.

k) V případě přijímání jakýchkoliv rozhodnutí, která se týkají ochrany osobních údajů, musí být Pověřenec fyzicky přítomen, aby mohl poskytnout svá stanoviska a posudky.

Článek 22
Povinnosti při zpracování OÚ

Pro zpracování OÚ v Organizaci platí následující povinnosti a pravidla:

22.1 Všichni zaměstnanci jsou povinni zachovávat mlčenlivost o veškerých informacích, se kterými byli obeznámeni v souvislosti se zpracováním OÚ. Povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo příslušných prací. Mlčenlivost se vztahuje i na opatření, která slouží k zabezpečení zpracování OÚ.

22.2 Zaměstnanci nesmí umožnit nahlížet do OÚ či předávat OÚ neoprávněným osobám.

22.3 Zaměstnancům je zakázáno bezdůvodně pořizovat kopie nebo videozáznamy (fotografie) OÚ, ani pořizovat kopie souborů obsahující OÚ.

22.4 U kopie dokumentu obsahující OÚ je potřeba uplatňovat stejná pravidla pro ochranu OÚ jako u originálu.

22.5 Zaměstnanci, kteří si pořídili kopii dokumentu obsahující OÚ výhradně pro pracovní potřebu, tuto kopii po skončení důvodu pro zpracování skartují či v případě elektronické kopie odstraní.

22.6 Všem zaměstnancům je zakázáno OÚ ukládat na vnitřních i externích paměťových médiích osobních počítačů a mobilních zařízeních. Výjimky schvaluje příslušná Odpovědná osoba. Adekvátní zajištění úložiště OÚ (např. šifrování), zajistí IT a ohlásí k zaevidování ZOÚ do seznamu úložišť.

22.7 Všem zaměstnancům je zakázáno zpracovávat OÚ na neschválených IT prostředcích.

22.8 Je zakázáno posílat dokumenty obsahující OÚ e-mailem mimo interní síť. V případě potřeby zaslání OÚ mimo interní síť Organizace, musí být přenos přiměřeně zajištěn, např. šifrováním dokumentu a dešifrovací klíč zaslat jiným distribučním kanálem, anebo použitím zabezpečeného kanálu (digitální certifikát).

22.9 Všechny odpovědné osoby v Organizaci jsou odpovědny za zpracování OÚ, jsou povinni přijmout takové opatření (v případě technických opatření ve spolupráci s příslušnými organizačními jednotkami), aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k OÚ, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití. Tato povinnost platí i po ukončení zpracování OÚ.

Článek 23
Technická a organizační opatření

23.1 Organizační a technická opatření:

a) Personální bezpečnost

S osobními údaji má možnost se seznámit pouze oprávněná osoba, a to v rozsahu odpovídajícímu jejímu oprávnění. Oprávnění této osoby vyplývá z její pracovní náplně na základě uzavřeného pracovněprávního vztahu nebo obdobného vztahu. Oprávněná osoba musí mít objektivní a důvodnou potřebu seznámit se s osobními údaji za účelem plnění pracovních povinností či jiných povinností nebo oprávněných zájmů.

b) Fyzická bezpečnost

Dokumenty s osobními údaji se ukládají na příslušných pracovištích (kanceláře, spisovna apod.) v souladu se Spisovým řádem a ostatními interními předpisy.

Dokumenty obsahující osobní údaje jsou ukládány tak, aby nedošlo ke zneužití osobních údajů, a to zejména uložením v uzamykatelných místnostech či v uzamykatelném nábytku, a to jak v průběhu, tak i po ukončení pracovní doby (pravidlo „čistého stolu“). – omezení přístupu neoprávněných osob v rámci pracovní doby, kteří nejsou oprávněni nakládat s osobními údaji uvedenými na dokumentech v listinné podobě.

Klíči od uzamčené schránky disponuje vlastník procesu nebo jím určená osoba. Duplikáty klíčů od uzamčené schránky jsou uloženy u přímého nadřízeného vlastníka procesu nebo jím určené osoby v zapečetěné obálce.

V době nepřítomnosti vlastníka procesu může uzamčenou schránku bez souhlasu odpovědné osoby otevřít pouze nejblíže nadřízený zaměstnanec vlastníka procesu nebo jím určená osoba.

Při skončení pracovněprávního vztahu vlastníka procesu zabezpečí předání údajů jiné osobě nejblíže nadřízený zaměstnanec vlastníka procesu. Pokud není přebírající znám, vlastník procesu předá dokumenty nejblíže nadřízenému zaměstnanci, nebo dokumenty uloží do spisovny Organizace v zabezpečeném obalu, ke kterému přiloží seznam ukládaných dokumentů.

Přístup k osobním údajům v listinné podobě je zabezpečen minimálně prostřednictvím mechanických zábranných prostředků (dveře, mříže, uzamykací systémy, uzamykatelný nábytek apod.), případně dalšími systémy technické ochrany (např. poplachovým zabezpečovacím systémem, dohledovým videosystémem, systémem kontroly vstupu apod.).

Významné prostory, kde dochází k dlouhodobému ukládání osobních údajů v listinné podobě (např. archivy, sklady, spisovny apod.) jsou zabezpečeny podle předcházejícího odstavce a jsou přístupné výhradně osobám pověřeným ředitelem organizace.

c) Informační bezpečnost osobních údajů ukládaných v ICT Organizace

Zabezpečení přístupu k osobním údajům zpracovávaných v ICT Organizace vychází z IT směrnic.

23.2 Organizace je povinna přijmout a dodržovat tato opatření v oblasti ochrany osobních údajů v dohledových videosystémech:

a) Osobní údaje, které jsou zpracovávány v rámci provozu dohledového videosystému jsou chráněny tak, aby nedošlo k jejich zneužití.

b) Dohledový videosystém je zabezpečen tak, aby k němu neměly přístup neoprávněné osoby a to tak, že jeho významné součásti (zejména záznamové zařízení, servery a jiná datová uložiště) jsou umístěny v zabezpečených prostorách, které jsou přístupné pouze osobám pověřeným ředitelem organizace.

c) Přístup k osobním údajům dohledového videosystému je zabezpečen prostřednictvím autentizace

a autorizace, tedy použitím přihlašovacího jména a hesla či jiným obdobným bezpečnostním prvkem.

d) Dohledový videosystém musí být chráněn antivirovým a antimalware softwarem, případně dalším bezpečnostním softwarem.

e) Data uložená v záznamovém zařízení dohledového videosystému jsou uchovávána po dobu nezbytně nutnou, která je stanovena na 7 dnů. (poznámka - jedná se o dobu odůvodnitelnou s ohledem na provozní potřeby konkrétní organizace). Doba uchování dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Tato doba by neměla přesáhnout v rámci časové smyčky např. 24 hodin, pokud se jedná o trvale střežený objekt, případně i dobu delší, nepřesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle zvláštního zákona, a po uplynutí této doby vymazána. V případech existujícího bezpečnostního incidentu by měla být data uložena po dobu nezbytně nutnou k předání orgánům činným v trestním řízení.

f) Aplikace a informační systém dohledového videosystému, ve kterých jsou zpracovávány osobní údaje, vytvářejí auditní záznamy, ohledně přístupu k osobním údajům jednotlivými koncovými uživateli, tak aby bylo možné zjistit, jaká osoba měla k osobním údajům přístup a v jakém rozsahu. Auditní záznamy jsou zabezpečeny proti jejich modifikacím.

g) Přístup osob do zařízení dohledového videosystému, informačního systému či aplikace dohledového videosystému, včetně přístupu do záznamového zařízení dohledového videosystému je umožněn pouze osobám, na základě schválení ředitele organizace či osoby pověřené ředitelem organizace.

h) Pořizování kopie záznamu dohledového videosystému je umožněn výhradně na základě schválení ředitele organizace a to pouze z odůvodnitelných důvodů (např. v případě zdokumentování okolností poškození zdraví osob či majetku organizace apod.).

i) Předání záznamu z dohledového videosystému je umožněn výhradně na základě schválení ředitele organizace (např. na základě písemné žádosti Policie České republiky) a předávacího protokolu, který je přílohou č. 3 této směrnice.

j) O instalaci dohledového videosystému jsou u vstupu do monitorovaných prostorů instalovány informační tabulky s příslušným textem, kterým je splněna informační povinnosti vůči subjektům údajů. Vzor informační tabulky je uveden v příloze č. 4 této směrnice.

Článek 24
Záznamy o činnostech zpracování

24.1 Pro každý účel zpracování OÚ v Organizaci musí být vypracován a veden Záznam o činnostech zpracování.

24.2 Za věcnou správnost jednotlivých Záznamů o činnostech zpracování je odpovědný ZOÚ, který zajišťuje, aby Záznamy o činnostech zpracování byly k dispozici v aktuální formě (elektronické a písemné, nebo jen písemné).

24.3 Evidenci všech Záznamů o činnostech zpracování vede ZOÚ.

24.4 Kontrola a aktualizace záznamů o činnostech zpracování se provádí 1x ročně. ZOÚ vyzve odpovědné osoby zasláním příslušných evidovaných Záznamů o činnostech zpracování k ověření jejich správnosti, aktuálnosti a případnému doplnění, včetně stanovení příslušných lhůt pro provedení kontroly.

Článek 25
Nové zpracování OÚ, změna stávajícího zpracování OÚ

25.1 Nové zpracování, či změnu stávajícího zpracování OÚ zajišťuje Odpovědná osoba při současném zohlednění zásad zpracování OÚ dle článku 4 této směrnice.

25.2 V případě nového zpracování či změny stávajícího zpracování OÚ je příslušná odpovědná osoba povinna vypracovat, či aktualizovat příslušný odpovědná osoba (v případě technických opatření ve spolupráci s příslušnými organizačními jednotkami – IT, Údržba aj.), a odeslat jej k vyjádření ZOÚ.

25.3 Na základě nového, či aktualizovaného Záznamu o činnostech zpracování provede ZOÚ vyhodnocení nutnosti DPIA, a v případě potřeby zajistí jeho realizaci.

25.4 ZOÚ zajistí ve spolupráci s odpovědnou osobou, IT a Údržbou posouzení rizik dopadu konkrétního zpracování na subjekty osobních údajů.

Článek 26
Likvidace osobních údajů

26.1 Po ukončení zpracování OÚ, nebo na základě oprávněné žádosti subjektu OÚ zajistí likvidaci OÚ příslušná odpovědná osoba.

26.2 Při likvidaci těchto údajů je nutné vyplnit Likvidační protokol, který musí být podepsán 2 oprávněnými zaměstnanci, které určí příslušná odpovědná osoba. Protokoly o likvidaci OÚ Odpovědná osoba nebo jím pověřený pracovník.

26.3 Likvidaci fyzických dokumentů zajišťuje příslušný pracovník (oprávněný pracovník za účasti druhého oprávněného pracovníka) skartováním.

26.4 Vymazání OÚ z úložišť a systémů zajišťuje IT.

Článek 27
Evidence úložišť OÚ

27.1 Evidenci úložišť OÚ v Organizaci vede ZOÚ.

27.2 Zabezpečení datových úložišť OÚ, např. dle bodu 3.14, písm. a) a b), zajišťuje IT.

27.3 Zabezpečení přenosných úložišť OÚ, např. dle bodu 3.14, písm. c) a d), zajišťuje příslušný zaměstnanec, kterému byly přiděleny.

27.4 Zabezpečení fyzických úložišť OÚ, např. dle bodu 3.14, písm. e), zajišťuje Údržba.

27.5 V případě změny nebo aktualizace zabezpečení úložišť zašle IT nebo Údržba požadavek na změnu, resp. aktualizaci k vyjádření ZOÚ a k provedení aktualizace Evidence úložišť.

27.6 ZOÚ následně ve spolupráci s příslušným garantem agendy provede aktualizaci Záznamů o činnostech zpracování.

Článek 28
Vyřízení požadavku subjektu údajů

28.1 Subjekt údajů je oprávněn žádat o:

a) Přístup k OÚ

b) Opravu OÚ

c) Výmaz OÚ

d) Omezení zpracování, vznést námitku

28.2 Tento postup je organizací využit v případě, kdy subjekt údajů, či jiná osoba vykonávající práva subjektu údajů (dále jen „žadatel“), uplatní prostřednictvím žádosti práva dle čl. 15 až 20 GDPR (dále jen „žádost“) vůči organizaci.

28.3 Za vyřízení žádosti odpovídá ZOÚ.

28.4 Práva má možnost žák/zákonný zástupce uplatnit u pověřence pro ochranu osobních údajů nebo přímo ve škole:

osobně na podatelně

elektronicky prostřednictvím datové schránky

e-mailem s elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném certifikační autoritou uznávanou v ČR.

28.5 Kopie zpracovávaných osobních údajů se poskytuje zdarma. Za zjevně nedůvodnou žádost bude požadována žádost, je-li osobou podána opakovaně. V takovém případě uloží za zpracování žádosti žáka/zákonného zástupce přiměřený poplatek nebo žádosti odmítne vyhovět. Totožnost žadatele je ověřena v případě, že žádost je ve fyzické podobě opatřena jasnými identifikačními údaji žadatele a jeho podpisem. Totožnost je také ověřena, pokud je žádost v elektronické podobě opatřena zaručeným elektronickým podpisem a nepanují pochybnosti o totožnosti žadatele. Totožnost žadatele je rovněž ověřena v případě, kdy byla žádost podána na podatelně. V případě, že je žádost podána elektronicky bez zaručeného elektronického podpisu a z okolností nevyplývá totožnost žadatele, je organizace povinna vyzvat žadatele k objasnění své totožnosti dle předchozí věty.

28.6 Pokud bude žadatel požadovat kopii osobních údajů ve smyslu čl. 15 odst. 3 GDPR, je žadatel povinen žádost podat s úředně ověřeným podpisem, elektronicky se zaručeným elektronickým podpisem, datovou schránkou nebo osobně po ověření totožnosti dle předchozího odstavce. Bez takového ověření nelze vydat kopie osobních údajů. Kopie osobních údajů budou vydávány do vlastních rukou žadatele.

28.7 Jestliže žádost obdrží kterýkoliv pracovník organizace, je povinen ji okamžitě postoupit řediteli organizace.

28.8 Po obdržení žádosti vyrozumí ředitel o této skutečnosti Pověřence, a to v následujícím rozsahu:

datum přijetí žádosti,

popis obsahu žádosti, tzn. které právo subjektu údajů dle je uplatňováno,

předpokládaný termín vyřízení žádosti.

28.9 V případě, kdy jsou podávány žádosti zjevně nedůvodné, nepřiměřeně či opakované, je organizace oprávněna žádost odmítnout. Odmítnutí musí být řádně odůvodněno.

Článek 29
Postup nahlášení bezpečnostního incidentu dle čl. 33 GDPR

29.1 Tento postup je organizací využit v případě, kdy je nutné dozorovému úřadu (tj. Úřadu pro ochranu osobních údajů) porušení zabezpečení osobních údajů dle čl. 33 a násl. GDPR (dále jen „bezpečnostní incident“).

29.2 Za oznámení bezpečnostního incidentu dozorovému úřadu odpovídá ředitel organizace.

29.3 Za bezpečnostní incident je považováno takové narušení zabezpečení osobních údajů, které by mohlo způsobit náhodné či protiprávní zničení, ztrátu, změnu, zpřístupnění či přenesení osobních údajů zpracovávaných organizací. Příkladem bezpečnostního incidentu může být např. odcizení dokumentů obsahujících osobní údaje, vážná porucha serveru atd.

29.4 Ihned po zjištění, nejpozději do 48 hodin, možného bezpečnostního incidentu ředitel kontaktuje Pověřence, se kterým zkonzultuje další postup.

29.5 Při kontaktu s Pověřencem (případně následně též s dozorovým úřadem) je povinností organizace, co nejpřesněji bezpečnostní incident popsat. Popis bezpečnostního incidentu musí obsahovat alespoň následující:

- popis povahy bezpečnostního incidentu (popis co a kde se stalo),
- uvedení data a hodiny vzniku či zjištění bezpečnostního incidentu (popis kdy se stalo),
- popis kategorií osobních údajů, které jsou bezpečnostním incidentem ohroženy (citlivé osobní údaje, osobní údaje nezletilých apod.),
- alespoň přibližný počet subjektů údajů, které mohou být bezpečnostním incidentem ohroženy (nelze-li určit přesně aspoň přibližný počet),
- popis případného rizika, které v souvislosti s bezpečnostním incidentem může vzniknout subjektům údajů.

29.6 Pověřenec (případně pověřenec Moravskoslezského kraje) provede vyhodnocení bezpečnostního incidentu; a to v rozsahu rizika nízkého, středního či vysokého. V případě vyhodnocení bezpečnostního incidentu jako vysoce rizikového, je nutné provést oznámení dozorovému úřadu dle čl. 33 GDPR vždy; v případě vyhodnocení bezpečnostního incidentu jako středně rizikového záleží na okolnostech případu a vyjádření pověřence (event. pověřence Moravskoslezského kraje), zda je nutné dozorovému úřadu incident ohlásit.

29.7 Ředitel organizace je povinen zajistit evidenci bezpečnostních incidentů v tomto rozsahu:

- datum a čas zjištění incidentu,
- datum a čas kontaktování pověřence,
- popis bezpečnostního incidentu dle odstavce 5 tohoto postupu,
- popis důsledků bezpečnostního incidentu,
- informace o posouzení rizika posouzení rizika pověřencem, příp. pověřencem Moravskoslezského kraje,
- popis případných přijatých opatření v souvislosti s řešením bezpečnostního incidentu,
- datum, čas a způsob případného ohlášení bezpečnostního incidentu dozorovému úřadu, případně subjektům osobních údajů dle č. 34 GDPR.

29.8 V případě, že je v souladu s odst. 6 tohoto postupu nezbytné ohlásit dozorovému úřadu bezpečnostní incident, bude toto ohlášení obsahovat následující:

popis povahy bezpečnostního incidentu (co kdy a kde se stalo),
kontaktní údaje pověřence pro ochranu osobních údajů (jméno, e-mail, telefon),
popis pravděpodobných důsledků bezpečnostního incidentu,
popis opatření, která již byla organizací přijata nebo jsou navržena k přijetí s cílem vyřešit daný bezpečnostní incident.

Článek 30
Uzavření smlouvy se zpracovateli OÚ

30.1 Přípravu smlouvy se zpracovatelem OÚ zajišťuje příslušný garant agendy ve spolupráci s příslušnými odbornými útvary Organizace a ZOÚ. Smlouva musí respektovat Článek 12 této směrnice.

30.2 ZOÚ ověřuje zapracování požadavků Článek 12 do smlouvy.

Článek 31
Vzdělávání

31.1 ZOÚ zajistí pravidelné vzdělávání zaměstnanců, kteří přichází do styku s osobními údaji.

Článek 32
Odpovědnost a povinnosti Správce při zpracování osobních údajů

32.1 Organizace jako Správce odpovídá za dodržování jednotlivých povinností stanovených právními předpisy upravujícími ochranu osobních údajů.

32.2 Organizace má definované role a odpovědnosti při zpracování osobních údajů v rámci své působnosti ustanovené pracovními náplněmi.

32.3 Organizace vystupuje převážně v roli Správce.

32.4 Zmocnění ke zpracování osobních údajů vyplývá ze zvláštního právního předpisu nebo ze smlouvy o zpracování osobních údajů, případně z uděleného Souhlasu od subjektu. Ve všech případech musí být dostatečným způsobem upraveny požadavky na vhodná technická a organizační opatření na ochranu osobních údajů.

32.5 Pokud se na zpracování osobních údajů v gesci Správce podílí třetí strana (Zpracovatel), pak Organizace smí využít pouze takového Zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky stanovené Nařízením a touto směrnicí a aby byla zajištěna ochrana práv subjektů. Smlouva o zpracování osobních údajů Zpracovatelem musí mít písemnou formu. Ve smlouvě musí být uveden předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva Správce, požadavky na vhodná technická a organizační opatření na ochranu osobních údajů, resp. záruky Zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů, jež má dle smlouvy zpracovat, a požadavky na poskytování součinnosti při ohlašování případů porušení zabezpečení osobních údajů úřadu. Smlouva musí obsahovat i další náležitosti stanovené v čl. 28 odst. 3 Nařízení.

32.6 Organizace v pozici Správce určuje účely a prostředky zpracování osobních údajů a nese za tuto činnost odpovědnost. Jestliže Organizace zjistí, že Zpracovatel porušuje povinnosti stanovené Nařízením, je povinna na tuto skutečnost Zpracovatele neprodleně upozornit a ukončit zpracování osobních údajů

Zpracovatelem.

32.7 Organizace jako Správce nebo Zpracovatel spolupracuje na požádání s úřadem při plnění jeho úkolů

Článek 33
Závěrečná ustanovení

33.1 Všichni vedoucí pracovníci jsou povinni prokazatelně (proti podpisu) seznámit s touto směrnicí zaměstnance jimi řízeného útvaru, kteří přicházejí do styku s osobními údaji.

33.2 Tato směrnice nabývá platnosti dne 25. 5. 2018.

33.3 Odborný výklad k této směrnici podá ZOÚ.

Přílohy:

Příloha č. 1 – Souhlas se zpracováním osobních údajů

Příloha č. 2 – Evidence souhlasů se zpracováním osobních údajů

Příloha č. 3 – Záznamy o činnostech zpracování

Příloha č. 4 – Posouzení rizik

Příloha č. 5 – Předávací protokol o předání záznamu z dohledového videosystému