Směrnice k zabezpečení ochrany osobních údajů

(technicko-organizační opatření k zajištění ochrany osobních údajů)

v organizaci

Dům dětí a mládeže Dobruška

Domašínská 363

518 01 Dobruška

IČ: 64224635

Článek I.
Úvodní ustanovení

Tato směrnice upravuje technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s NAŘÍZENÍM EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, 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), tzv. GDPR (dále jen „GDPR") a předpisů souvisících s cílem zajištění správné praxe při přijímání a realizaci opatření k ochraně osobních údajů (zejména zákona 110/2019 Sb.) v organizaci **Dům dětí a mládeže Dobruška, Domašínská 363, Dobruška 51801, IČ: 64224635** (dále jen „organizace").

Článek II.
Působnost

(1) Touto směrnicí jsou vázáni všichni členové statutárních orgánů organizace, zaměstnanci, pracovníci i další osoby, které přicházejí do styku s osobními údaji v organizaci, nebo v rámci své práce pro organizaci.

(2) Tato směrnice platí přiměřeně i pro společnosti či organizace, přicházející do styku s osobními údaji v organizaci, nebo v rámci své práce pro organizaci, případně také pro dceřiné subjekty organizace či jiné právnické osoby ovládané nebo zřízené organizací.

(3) Pokud organizace provádí svoji činnost na území jiného státu, je povinna dodržovat i pravidla pro ochranu osobních údajů platná v takovém státu.

Článek III.
Vymezení pojmů

Pro účely této směrnice se rozumí:

a) **archivace** – uchování informací v listinné, či elektronické podobě;

b) **bezpečnost zpracování osobních údajů** – technická a organizační opatření, zajišťující úroveň zabezpečení odpovídající danému riziku;

c) **biometrické údaje** – 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, daktyloskopické údaje (otisky prstů), obraz krevního řečiště, biomechanika chůze, obraz sítnice oka, a podobně;

d) **citlivý údaj** – neboli zvláštní kategorie osobních údajů, je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů, genetický údaj subjektu údajů či biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci (proces ověření skutečné identity osoby) subjektu údajů;

e) **genetické údaje** – osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;

f) **likvidace osobních údajů** – fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování;
g) **osobní údaj** – jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, přičemž subjekt údajů se považuje za určený nebo určitelný, jestliže jej lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu, tedy jakékoli údaje, podle kterých je možné přímo, či nepřímo identifikovat konkrétního člověka (zpravidla jméno, příjmení, adresa, rodné číslo, fotografie, apod.);
h) **příjemce** – každý subjekt, kterému jsou osobní údaje zpřístupněny;
i) **pseudonymizace osobních údajů** – proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost;
j) **shromažďování 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) **souhlas subjektu údajů** – svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů;
l) **správce** – každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj (zpracováním osobních údajů může správce pověřit zpracovatele);
m) **subjekt údajů** – fyzická osoba, k níž se osobní údaje vztahují;
n) **uchovávání osobních údajů** – udržování údajů v takové podobě, která je umožňuje dále zpracovávat;
o) **zpracování osobních údajů** – jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, jako je např. shromažďování, ukládání na nosiče, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace osobních údajů;
p) **zpracovatel** – každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona;
r) **zveřejněný osobním údajem** – osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Článek IV.
Povinnosti osob při správě a zpracování osobních údajů

(1) Vedení organizace v rámci své odpovědnosti za ochranu osobních údajů, samo, nebo prostřednictvím pověřených osob:
   a) zajišťuje podmínky pro řádnou ochranu osobních údajů, ve smyslu GDPR a ostatních právních předpisů, včetně příslušné legislativy Evropské unie;
   b) zajišťuje průběžné vzdělávání zaměstnanců v oblasti ochrany osobních údajů, a to v první řadě formou jejich samostudia, v případě potřeby formou školení, či konzultací;
   c) odpovídá za personální zajištění ochrany osobních údajů;

d) zajišťuje zdroje informací ke správné praxi při ochraně osobních údajů, včetně kontaktů na osoby odborně schopné konzultovat předmětnou problematiku, případně na pověřence pro ochranu osobních údajů, pokud je jmenován;
e) zajišťuje kontrolu činnosti při ochraně osobních údajů;
f) zajišťuje realizaci opatření v oblasti ochrany osobních údajů, včetně znalosti povinností osob přicházejících do styku s osobními údaji;
g) v případě potřeby provádí posouzení dopadu činnosti na ochranu osobních údajů,
h) v případě potřeby provádí předběžné konzultace s Úřadem pro ochranu osobních údajů (dále jen ÚOOÚ);
i) vede záznamy o zpracováních osobních údajů;
j) ohlašuje případy narušení bezpečnosti osobních údajů do 72 h od doby, kdy se jako správce o narušení dozví, na ÚOOÚ a pokud je to třeba i dotčeným osobám, o jejichž osobní údaje se jednalo;
k) umožní přenositelnost osobních údajů k jinému správci ve vhodném formátu;
l) v případě potřeby jmenuje pověřence pro ochranu osobních údajů;
m) plní pokyny dozorových orgánů v oblasti ochrany osobních údajů.

(2) Osoby přicházející do styku s osobními údaji jsou povinny:
a) zpracovávat osobní údaje v souladu s GDPR a příslušnými zákony, ostatními právními normami, jakož i dalšími předpisy EU a mezinárodními smlouvami, které se na tuto problematiku při jejich práci vztahují;
b) zachovávat mlčenlivost o osobních údajích a přijatých opatřeních k jejich ochraně, a to i po skončení svého pracovněprávního nebo smluvního vztahu u organizace;
c) zabránit neoprávněnému čtení, pozměnění, smazání, či znepřístupnění osobních údajů, nevytvářet kopie software nebo listin s osobními údaji pro jinou než pracovní potřebu a nepřipustit takové jednání ani jiným osobám, například tím, že nebude možné z nosičů či úložišť počítačových dat kopírovat na jiné nosiče větší množství osobních údajů bez toho, že by toto kopírování schválilo a zároveň i technicky umožnilo (např. zadáním hesel) současně dvě nebo více osob;
d) při používání výpočetní techniky používat pouze bezpečný hardware a software, a to bezpečným způsobem a bezodkladně hlásit veškeré nestandardní projevy používané výpočetní techniky příslušným odborníkům;
e) dodržovat zásady bezpečného používání výpočetní techniky zejména používáním vhodných hesel a dbát na jejich ochranu před prozrazením; nenavštěvovat rizikové webové stránky apod., okamžitě hlásit jakékoli důvodné podezření na ohrožení bezpečnosti osobních údajů.

Článek V.
Technická opatření k zajištění ochrany osobních údajů

(1) Písemnosti a jiné hmotné nosiče dat, které obsahují osobní údaje, je možné uchovávat pouze v uzamykatelných místnostech a pokud možno i uzamykatelných skříních. Mimo uzamykatelné

místnosti lze mít písemnosti a jiné hmotné nosiče dat, které obsahují osobní údaje, uloženy např. na chodbách, jen za podmínky, že se jedná o chodby, kam nemají volný přístup jiné osoby než zaměstnanci organizace a tyto skříně jsou trvale uzamčeny vhodnými zámky a jsou konstruovány tak, aby je nebylo možné snadno vypáčit, či jinak do nich snadno vniknout násilím. Podrobnější pokyny k uzamykání místností a skříní, jakož i k přidělování, ukládání a výrobě klíčů vydávají dle potřeby vedoucí pracovníci příslušných útvarů a pracovišť, a to obvykle jednotlivým zaměstnancům, zpravidla při jejich nástupu do pracovního poměru, nebo přechodu na nové pracoviště.

(2) Elektronické datové soubory obsahující osobní údaje je možné uchovávat v paměti počítače pouze:

a) je-li přístup k takovýmto souborům chráněn doménovým jménem, které umožní zpětně zjistit, kdo měl k osobním údajům přístup a komu byly osobní údaje případně předány a heslem, které musí mít nejméně 6 znaků, z nichž alespoň jeden musí mít podobu čísla nebo znaku (přiměřené heslo);
b) je-li přístup k užívání počítače, v jehož paměti jsou tyto soubory umístěny, chráněn přiměřeným heslem (softwarovým či hardwarovým) nebo vhodným zámkem;
c) tak, že veškerá data musí být pravidelně zálohována a zálohová média musí být v přiměřených intervalech měněna, přičemž musí být zabráněno neoprávněnému přístupu k datovým nosičům;
d) tak, aby příslušné osoby měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, přičemž tato uživatelská oprávnění uděluje vedoucí příslušného pracoviště, nebo členové nejvyššího vedení organizace.

Podrobné pokyny k ochraně datových souborů (včetně hardware, které využívají) a k přidělování, ukládání a tvorbě domén, hesel a dalších ochranných prvků, obsahuje chráněná doložka k této směrnici, k níž mají přístup jen pověřené osoby uvedené v chráněné doložce.

(3) Osobní údaje, které nejsou v elektronické podobě, musí být chráněny v uzamykatelných místnostech, případně i uzamykatelných skříních, od nichž mají klíče jen pověřené osoby, které je nesmí zpřístupnit žádným nepovolaným osobám. Tam, kde se pracuje s citlivými údaji, musí být citlivé osobní údaje zabezpečeny zvlášť důkladně a musí být minimalizován okruh osob, které k nim mohou mít přístup.

(4) Veškeré listiny a jednorázově použitelné datové nosiče i jiné jednorázově použitelné materiály obsahující osobní údaje, musí být poté, co skončí důvody pro uchovávání osobních údajů, které se na nich nalézají, zničeny, či jinak zlikvidovány, pod dohledem osoby určené organizací. Pokud likvidaci listin, datových nosičů, či jiných materiálů obsahujících osobní údaje, provádí pracovník (zaměstnanec, či externí pracovník) organizace, musí být u takové činnosti přítomny nejméně dvě osoby, které nejsou vzájemně osobami blízkými. Při likvidaci většího množství písemností a jiných hmotných nosičů dat, které obsahují osobní údaje, se sepisuje likvidační protokol, ve kterém se uvede datum, místo likvidace a její způsob; stejně se postupuje při likvidaci listin, datových nosičů, či jiných materiálů obsahujících citlivé osobní

údaje. Likvidace osobních údajů na opakovatelně použitelných nosičích se provádí tak, aby je nebylo možno ani zpětně obnovit (nosiče není třeba ničit), přičemž i v tomto případě musí být likvidaci přítomny nejméně dvě osoby, které nejsou vzájemně osobami blízkými. V případě likvidace listin, datových nosičů, či jiných materiálů obsahujících osobní údaje externí organizace musí být prováděna alespoň občasná namátková kontrola zástupcem organizace nebo jinou pověřenou osobou.

(5) Tzv. citlivé osobní údaje musí být uchovávány, jen pokud je to nezbytné k plnění zákonných povinností a musí být chráněny zvláště pečlivě před přístupem třetím osobám. Přesnější pokyny k ochraně citlivých osobních údajů, mohou být podrobněji upraveny v jiných interních dokumentech organizace. Tam, kde není zřejmé, že se citlivé osobní údaje shromažďují na základě zákona, musí být získány i kvalifikované souhlasy se zpracováním těchto citlivých osobních údajů od příslušných subjektů údajů, nebo jejich zákonných zástupců.

(6) Veškeré kamerové, či audio záznamy, musí být pořizovány jen v souladu s příslušnými právními předpisy, veškeré kamery a ukládání záznamů z těchto kamer, musí být posouzeny z hlediska jejich dopadu na ochranu osobních údajů. Záznamy z těchto kamer musí být kódovány a ve formě tzv. černé skříňky musí být uloženy mimo dosah nepovolaných osob. Pokud není důvodná potřeba delšího uchování, např. jako důkaz pro pozdější právní úkony, musí být kamerové záznamy mazány nejpozději ve lhůtách přiměřených účelu jejich ukládání. Tam, kde jsou kamery umístěny i z důvodu bezpečnosti a ochrany zdraví při práci, včetně využití pro náhradu škody zaměstnanci, se považuje **lhůta pro vymazání kamerových záznamů** za přiměřenou, pokud jsou kamerové záznamy vymazány nejpozději do **14 dnů od jejich pořízení**, a to vzhledem ke lhůtám, ve kterých jsou zaměstnanci povinni hlásit zaměstnavateli vznik škody podle zákoníku práce.

(7) Žádné kamerové, či audio záznamy, nesmí být pořizovány tam, kde by mohly urážet lidskou důstojnost nebo zvyšovat nebezpečí úrazu či vzniku škody.

(8) O umístění kamer nebo pořizování audiozáznamů musí být všechny osoby řádně informovány informačními tabulkami, či jiným vhodným způsobem, včetně informace, kde mohou získat o takových záznamech podrobnější informace.

(9) Podrobné pokyny k technickým a organizačním opatřením na ochranu kamerových záznamů před ztrátou, zničením nebo zneužitím, mohou být upraveny v chráněné doložce k této směrnici, k níž budou mít přístup jen pověřené osoby uvedené v takové chráněné doložce.

Článek VI.
Posouzení dopadu činnosti na ochranu osobních údajů

(1) Pokud je pravděpodobné, že určitý druh zpracování osobních údajů v organizaci, nebo u jejího zpracovatele, zejména při využití nových (počítačových) technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a

svobody fyzických osob, vypracuje organizace posouzení dopadu své činnosti na ochranu osobních údajů. Posouzení dopadu činnosti na ochranu osobních údajů musí obsahovat systematický popis zamýšleného zpracování, posouzení rizik, provedení testu proporcionality a podobně. V posouzení dopadu činnosti na ochranu osobních údajů musí být také jasně definována přijatá bezpečností opatření a záruky k ochraně osobních údajů.

(2) Vedoucí pracovníci organizace jsou povinni především zkoumat, zda v organizaci není prováděno 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. Zejména jsou povinni zkoumat, zda nejsou podle výpočetní techniky, zvláště pak v případě využití umělé inteligence, zaměstnanci, zákazníci, či jiné osoby, tříděny do určitých skupin a v důsledku takového roztřídění do skupin, zda pak nejsou bez konečného rozhodnutí člověka určována jejich práva, či povinnosti (např. rozhodování o změně pracovního zařazení, o výši mzdy, či benefitů, o skončení pracovního poměru a podobně).

(3) Vedoucí pracovníci organizace jsou také povinni zkoumat, zda v organizaci není prováděno rozsáhlé zpracování zvláštních kategorií údajů (citlivých údajů, včetně biometrických), nebo rozsáhlé systematické monitorování veřejně přístupných prostorů, např. kamerovými systémy.

(4) Vzhledem k tomu, že podle znalostí provozu v organizaci nedochází ani ke zpracování osobních údajů způsobem uvedeným v čl. VI/2, ani není prováděno rozsáhlé zpracování zvláštních kategorií údajů (citlivých údajů, včetně biometrických), není v organizaci v tomto směru vysoké riziko pro práva a svobody fyzických osob. Pokud se jedná o rozsáhlé systematické monitorování veřejně přístupných prostorů kamerovými systémy, tím, že organizace dodržuje zásady uvedené v čl. VI/6 až VI/9, není ani toto zpracování osobních údajů vysokým rizikem pro práva a svobody fyzických osob.

Článek VII.
Konzultace s Úřadem pro ochranu osobních údajů

Vzhledem k tomu, že v rámci posouzení dopadu činnosti organizace na ochranu osobních údajů nebylo zjištěno, že by určitý druh zpracování osobních údajů v organizaci, nebo u jejího zpracovatele, zejména při využití nových (počítačových) technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování osobních údajů, mohl mít za následek vysoké riziko pro práva a svobody fyzických osob, v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, jsou vedoucí pracovníci organizace povinni sledovat, zda nedošlo ke změně těchto poměrů v organizaci. Pokud by v souvislosti se změnami zpracování osobních údajů v organizaci došlo k situaci, že by vzniklo vysoké riziko pro práva a svobody fyzických osob a nebylo by známo, jaká přijmout opatření ke zmírnění tohoto rizika, jsou vedoucí pracovníci organizace povinni zajistit,

aby byla provedena předchozí konzultace řešení takového stavu s Úřadem pro ochranu osobních údajů.

Článek VIII.
Povinnost vést záznamy o činnostech zpracování osobních údajů

(1) Vedoucí pracovníci organizace jsou povinni zajistit, aby byly o veškerém zpracování osobních údajů vedeny záznamy, na základě kterých bude možné kdykoli doložit, kdo byl jejich správcem (jméno, příjmení a kontaktní údaje), případně kdo vystupoval jako pověřenec pro ochranu osobních údajů, účely zpracování osobních údajů, popis kategorií subjektů údajů a kategorií osobních údajů, kategorie příjemců, včetně příjemců ve třetích zemích nebo mezinárodních organizacích, informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, doložení vhodných záruk ochrany osobních údajů, plánované lhůty pro výmaz jednotlivých kategorií osobních údajů (podle skartačních předpisů), obecný popis technických a organizačních bezpečnostních opatření.

(2) Vedení záznamů o zpracování osobních údajů je možné provádět jak v elektronické, tak i papírové podobě. Záruky ochrany osobních údajů vyplývají z této směrnice, ve které je i obecný popis technických a organizačních bezpečnostních opatření.

(3) Pokud si organizace nechává zpracovávat osobní údaje od jiné osoby, je povinností vedoucích pracovníků společníků zajistit, aby byly osobní údaje zpracovávány na základě řádně uzavřené smlouvy o zpracování osobních údajů.

Článek IX.
Povinnost ohlašovat případy narušení bezpečnosti osobních údajů

(1) Vedoucí pracovníci organizace jsou povinni zajistit, aby byly veškeré případy narušení bezpečnosti osobních údajů nahlášeny Úřadu pro ochranu osobních údajů do 72 h od doby, kdy se jako organizace správce o takovém narušení dozví. Při tom jsou povinni zajistit, aby bylo řádně rozlišeno, zda se jedná skutečně o narušení bezpečnosti osobních údajů, či zda je riziko pro ochranu osobních údajů v takovém případě bezvýznamné.

(2) Pokud hrotí bezprostřední riziko pro práva subjektů údajů, jsou vedoucí pracovníci organizace povinni zajistit i to, aby tyto osoby byly také přiměřeným způsobem informovány o rizicích spojených s předmětným narušením bezpečnosti osobních údajů a byly jim poskytnuty i vhodné informace, jak případné hrozící škodě zabránit, nebo ji alespoň minimalizovat.

(3) Pokud došlo k narušení bezpečnosti osobních údajů, je třeba předtím, než bude taková skutečnost nahlášena Úřadu pro ochranu osobních údajů, řádně zanalyzovat situaci, vyhodnotit míru rizika pro organizaci i subjekty, připravit a spustit nápravná opatření a připravit plán oznámení dotčeným osobám. Teprve pak je vhodné oznámit Úřadu pro ochranu

osobních údajů, co se událo, včetně informace, co již bylo provedeno k minimalizaci škod a jaké kroky budou provedeny do budoucna.

(4) Dojde-li k narušení bezpečnosti osobních údajů je nutno nejprve odstranit zdroj porušení ochrany osobních údajů, poté musí být provedena informace dle předchozích odstavců tohoto článku.

(5) Je-li jmenován v organizaci pověřenec pro ochranu osobních údajů, veškeré kroky týkající se reakce na narušení ochrany osobních údajů, musí být konzultovány s tímto pověřencem pro ochranu osobních údajů a tam kde je to možné, prováděny jeho prostřednictvím.

Článek X.
Přenositelnost osobních údajů

(1) Vedoucí pracovníci organizace jsou povinni zajistit, aby byly veškeré osobní údaje, jejichž zpracování je založeno na souhlasu nebo na smlouvě a jejichž zpracování se provádí automatizovaně, přenositelné k jinému správci. S právem přenositelnosti je třeba počítat již dopředu a zpracování osobních údajů by mělo být pro správce prováděno takovým způsobem, aby při přenosu osobních údajů na nového zpracovatele bylo v maximální možné míře eliminováno rozkrytí systému práce organizace, prozrazení svých obchodních tajemství anebo obchodní strategie.

(2) Vedoucí pracovníci organizace jsou povinni také zajistit, aby při přenosu osobních údajů konkrétní osoby k jinému správci nebyla nepříznivě dotčena práva a svobody jiných osob, nebo práva duševního vlastnictví.

(3) Na přenositelnost osobních údajů musí být subjekt údajů výslovně upozorněn a toto právo musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací již v okamžiku první komunikace se subjektem údajů, tedy s osobami, jejichž osobní údaje mají být zpracovávány.

Článek XI.
Výmaz osobních údajů a právo na zapomenutí

(1) Vedoucí pracovníci organizace jsou povinni zajistit, aby byly veškeré osobní údaje, jejichž shromažďování, uchovávání, či zpracování není nezbytné pro plnění právních povinností správce, či zpracovatele, nebo pro ochranu jejich oprávněných zájmů, byly vymazány bez zbytečného odkladu poté, co o to jejich subjekt údajů formálně požádá. Za obdobných podmínek jsou vedoucí pracovníci povinni zajistit, aby byly subjekty údajů tzv. zapomenuty z hlediska jejich osobních údajů, pokud o zapomenutí formálně požádají. Tam, kde není možné jejich osobní údaje vymazat, protože se dostaly do vlivu jiné osoby z veřejných zdrojů, učiní správce i zpracovatel alespoň taková opatření, aby pokud je to možné, ztížil jejich nalezení. S právem na výmaz je třeba počítat již dopředu a zpracování osobních údajů by mělo

být pro správce prováděno takovým způsobem, aby osobní údaje, které by neměly být vymazány, byly již předem řádně identifikovány a případně uloženy zvlášť.

(2) Vedoucí pracovníci organizace jsou povinni také zajistit, aby při výmazu osobních údajů konkrétní osoby nebyla nepříznivě dotčena práva a svobody jiných osob.

Článek XII.
Pověřenec pro ochranu osobních údajů

(1) V případě, že jsou k tomu splněny podmínky, je povinností nejvyššího vedení organizace jmenovat pověřence pro ochranu osobních údajů.

(2) Pokud by byl jmenován pověřenec pro ochranu osobních údajů, ať již proto, že organizace naplňuje podmínky pro jeho povinné jmenování, nebo proto, že jej organizace jmenovala dobrovolně, bude se činnost pověřence pro ochranu osobních údajů řídit samostatnou speciální směrnicí.

(3) Pokud není pověřenec pro ochranu osobních údajů jmenován, vždy musí nejvyšší vedení organizace zajistit, aby měla organizace osobu, která je zodpovědná za plnění povinností v oblasti ochrany osobních údajů.

Článek XIII.
Předávání osobních údajů do zahraničí

(1) Pokud je nezbytné předávat osobní údaje do zahraničí, je povinností vedoucích pracovníků organizace zajistit, aby byly takové osobní údaje předávány jen vhodným a spolehlivým obchodním partnerům, aby bylo před předáním osobních údajů do zahraničí řádně prozkoumáno právního prostředí v zemi smluvního partnera, včetně ověření, zda existují mezinárodní smlouvy se zemí obchodního partnera na ochranu osobních údajů.

(2) Při předávání osobních údajů do zahraničí musí být vždy na takové předání uzavřena příslušná smlouvy s obchodním partnerem, která bude řešit i ochranu osobních údajů, včetně sankcí za její porušení.

Článek XIV.
Internetové obchodování a věrnostní systémy

(1) Pokud má organizace internetový obchod, nebo jakékoli prezentace své činnosti na internetu, je povinností vedoucích pracovníků organizace zajistit, aby na internetových stránkách organizace byli případní návštěvníci těchto webových stránek řádně informováni o svých právech a povinnostech. Zejména zde musí být uvedeny informace o podmínkách zpracování osobních údajů, o používání cookies, a podobně.

(2) Jestliže jsou na webových stránkách vyžadovány jakékoli souhlasy se zpracováním osobních údajů, musí být takový souhlas získáván vždy zásadně svobodně, informovaně, nikoli lstí a transparentně, tedy tak, aby každý, kdo uděluje souhlas se zpracováním svých osobních údajů, nebyl za neudělení takové souhlasu nijak potrestán. Jsou-li na webových stránkách pro udělení souhlasu zaškrtávací políčka, musí být tato políčka nastavena tak, že jednotlivé položky osoby zaškrtávají, nikoli že by rušily již předem provedené zaškrtnutí.

(3) U veškerých žádostí o souhlas se zpracováním osobních údajů musí být uvedeno, že tento souhlas je odvolatelný. Veškerá poučení týkající se souhlasu se zpracováním osobních údajů musí být napsána srozumitelným, jednoduchým jazykem.

(4) To, co je uvedeno v čl. XIV/1 až XIV/3, použije se přiměřeně i na souhlasy se zpracováním osobních údajů mimo internetovou, či jinou elektronickou komunikaci.

(5) Pokud má organizace zavedeny jakékoli věrnostní systémy, platí pro ně obdobná pravidla, jako pro výše uvedená pravidla při internetovém obchodování. Vždy musí být zajištěno, že osobní údaje jsou v rámci věrnostních systémů (tedy věrnostních karet, věrnostních programů nevyužívajících věrnostních karet, a podobně), řádně chráněny proti přístupu nepovolaných osob, subjekt údajů může kdykoli svoji účast ve věrnostním programu ukončit s tím, že zůstanou zachovány jen informace, které je organizace povinna uchovávat ze zákona (např. k prokázání skutečností, které je povinna doložit finančnímu úřadu).

(6) Nebrání-li tomu jiné zákonné důvody, pak pro zpracování osobních údajů účastníků věrnostních programů osob mladších 15 let je nezbytný souhlas jejich zákonných zástupců. Věková hranice 15 let platí i pro souhlasy se zpracováním osobních údajů pro jiné účely, než jsou věrnostní systémy.

(7) Má-li být věrnostní systém, do kterého je zapojena konkrétní osoba, užíván více osobami např. z její domácnosti, musí se tak vždy dít jen se souhlasem takového účastníka věrnostního programu.

(8) Jakékoli informace o osobních údajích účastníků věrnostních systémů mohou být zveřejněny jen se souhlasem subjektů údajů.

Článek XV.
Závěrečná ustanovení

(1) Jednotlivá opatření podle této směrnice mohou být podrobněji rozpracována ve specializovaných směrnicích, pokynech, nebo jiných relevantních dokumentech organizace.

Otázky neupravené touto směrnicí se řídí obecně závaznými právními předpisy, a to jako českými, tak i předpisy Evropské unie, včetně doporučení.

(2) Vedoucí pracovníci organizace jsou povinni zajistit, aby organizace řádně a včas komunikovala s Úřadem pro ochranu osobních údajů, a aby bylo o komunikaci s Úřadem pro ochranu osobních údajů vždy řádně a včas informováno nejvyšší vedení organizace.

(3) Tato směrnice nabývá účinnosti dnem 25. května 2018.

(4) Jakékoli změny této směrnice je možné činit jen ve formě číslovaných dodatků.

V Praze dne 25. května 2018

Aktualizace k 1. září 2024

Jitka Macková
ředitelka
Dům dětí a mládeže Dobruška