Nadační fond Arnošta Lustiga: GDPR směrnice

1. Všeobecná ustanovení

1.1. Úvodní ustanovení

Tato směrnice upravuje technická a 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 souvisejících s cílem zajištění správné praxe při přijímání a realizaci opatření k ochraně osobních údajů u osoby: Nadační fond Arnošta Lustiga IČO: 09549609, se sídlem Drtinova 557/10, Smíchov, 150 00 Praha 5 (dále jen „Fond“).

1.2. Rozsah působnosti

a) Touto směrnicí jsou vázáni všichni členové statutárních orgánů Fondu, zaměstnanci, pracovníci i další osoby,

které přicházejí do styku s osobními údaji ve Fondu, nebo v rámci své práce pro Fond.

b) Tato směrnice platí přiměřeně i pro třetí osoby, přicházející do styku s osobními údaji v rámci své činnosti pro Fond.

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

1.3. 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 sub-

jektu 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;

q) **zveřejněný osobním údajem** – osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

2. Povinnosti při správě a zpracování osobních údajů

2.1. Ředitel fondu

Ředitel Fondu sám 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 dotčených osob 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 zpracování 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.

2.2. Ostatní osoby přicházející do styku s osobními údaji

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 s Fondem;

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.

3. Technická opatření k zajištění ochrany osobních údajů

3.1. Uchovávání dat

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

3.2. Elektronické datové soubory

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.

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.

3.3. Listinné nosiče dat

a) 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).

b) 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. 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).

4. Posouzení dopadu činnosti na ochranu osobních údajů

4.1. Pokud je pravděpodobné, že určitý druh zpracování osobních údajů Fondem, 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 Fond 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.

4.2. Ředitel je povinen především zkoumat, zda ve Fondu 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 je povinna 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 člo-

věka určována jejich práva, či povinnosti (např. rozhodování o změně pracovního zařazení, o výši mzdy, či benefitů, o skončení pracovního poměru a podobně).

5. Povinnost vést záznamy o činnostech zpracování osobních údajů

5.1. Ředitel je povinen 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.

5.2. Vedení záznamů o zpracování osobních údajů je možné provádět jak v elektronické, tak i papírové podobě.

5.3. Pokud si Fond nechává zpracovávat osobní údaje od jiné osoby, zajistí Fond, aby byly osobní údaje zpracovávány na základě řádně uzavřené smlouvy o zpracování osobních údajů.

6. Povinnost ohlašovat případy narušení bezpečnosti osobních údajů

Ředitel je povinen zajistit, aby byly veškeré případy narušení bezpečnosti osobních údajů nahlášeny Úřadu pro ochranu

osobních údajů do 72 h od doby, kdy se 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.

7. Přenositelnost osobních údajů

7.1. Ředitel je povinen 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.

7.2. Ředitel je povinen také zajistit, aby při přenosu osobních údajů konkrétní osoby k jinému správci nebyla nepříznivě dotčena práva a svobody jiných osob, nebo práva duševního vlastnictví.

7.3. 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.

8. Výmaz osobních údajů a právo na zapomenutí

8.1. Ředitel je povinen zajistit, aby byly bez zbytečného odkladu vymazány veškeré osobní údaje, pokud:

a) osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.

b) subjekt údajů odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování.

c) osobní údaje byly zpracovány protiprávně.

d) pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí v souvislosti s nabídkou služeb informační společnosti.

8.2. Ředitel je povinen také zajistit, aby byly provedeny přiměřené kroky, včetně technických opatření k vymazání veškerých osobních údajů, včetně záloh a automatických obnov IT systémů.

9. Předávání osobních údajů do zahraničí

9.1. Pokud je nezbytné předávat osobní údaje do zahraničí, je Fond povinen 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.

9.2. 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).

10. Elektronická komunikace

10.1. Pokud má Fond jakoukoliv prezentaci své činnosti na internetu, je povinností Fondu zajistit, aby na internetových stránkách Fondu 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.

10.2. 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.

10.3. 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.

11. Závěrečná ustanovení

11.1. Jednotlivá opatření podle této směrnice mohou být podrobněji rozpracována ve specializovaných směrnicích, pokynech, nebo jiných relevantních dokumentech Fondu. Otázky neupravené touto směrnicí se řídí obecně závaznými právními předpisy, a to jako českými, tak u předpisy Evropské unie, včetně doporučení.

11.2. Tato směrnice nabývá účinnosti dnem 16. 6. 2021.

11.3. Jakékoli změny či doplnění této směrnice schvaluje správní rada Fondu, případně pověřený člen představenstva.