Interní směrnice o ochraně osobních údajů

1. Úvod

1.1 *Předmět a účel*

Tato interní směrnice o ochraně osobních údajů představuje jedno z technickoorganizačních opatření Správce (dále jen „Artlingua“) k zajištění ochrany osobních údajů v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“) a s dalšími právními předpisy.

1.2 *Pojmy*

1.2.1 *Osobní údaj*

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo nebo nepřímo identifikovat, zejména s 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.

1.2.2 *Citlivý osobní údaj*

Citlivým osobním údajem je údaj, který vypovídá o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

1.2.3 *Subjekt údajů*

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují. V souvislosti s činností Správce (Artlingua) jím je zpravidla klient společnosti nebo její zaměstnanec – fyzická osoba, zákazník nebo jiná fyzická osoba.

1.2.4 *Zpracování osobních údajů*

Zpracování osobních údajů je jakákoliv operace nebo soubor operací s osobními údaji nebo se soubory osobních údajů, která je prováděna pomocí či bez pomoci automatizovaných postupů. Příklady zpracování osobních údajů je sběr osobních údajů, jejich zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Správce zejména shromažďuje a ukládá osobní údaje zákazníků a zaměstnanců, a některé předává k dalšímu zpracování za účelem mzdové a účetní agendy. Subjektem, který tuto činnost provozuje je Mgr. Andrea Peláková, Podnikající pod IČ: 45731373, Zapsaná na seznamu daňových poradců pod číslem 2830, Praha 1, Národní 339/11, 100 00, DIČ: CZ6757170310.

1.2.5 *Likvidace osobních údajů*

Za likvidaci údajů se považuje fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení ze zpracování. Likvidace se provádí podle spisového a skartačního řádu Správce. Pověřený pracovník je povinen zařadit do skartačního řízení i dokumenty v elektronické formě.

1.2.6 *Správce*

Správcem je fyzická nebo právnická osoba, která určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak. Správcem je společnost ArtLingua.

1.2.7 *Zpracovatel*

Zpracovatelem je fyzická nebo právnická osoba nebo jiný subjekt, který zpracovává osobní údaje pro správce, tzn. sama neurčuje účel a prostředky zpracování. Zpracovateli se pro účely této směrnice rozumí též poskytovatelé informačních systémů, kteří mají oprávnění přístupu k osobním údajům (např. za účelem zajištění servisu či aktualizace software).

1.2.8 *Souhlas*

Souhlasem subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Souhlas je v prostředí Správcem doplňkovým institutem, a tvorbu souhlasů je v odpovídajících případech třeba konzultovat s pověřencem pro ochranu osobních údajů nebo s UOOÚ ČR.

1.2.9 *Zaměstnanec*

Zaměstnancem se pro účely této směrnice rozumí každý pracovník, který vykonává činnost pro Správce na základě pracovní smlouvy, dohody o pracovní činnosti nebo dohody o provedení práce. Tato směrnice se také v přiměřené míře vztahuje na jiné osoby, které zpracovávají pro Správce osobní údaje (např. Účetní subjekt) pokud byly s touto směrnicí seznámeni.

1.3 *Zkratky*

Správce	Artlingua, a.s.
ÚOOÚ	Úřad pro ochranu osobních údajů
GDPR	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 údajů a o zrušení směrnice 95/46/ES
EU	Evropská unie
ICT	Informační a komunikační technologie

2. Oprávněné osoby

2.1 Pravomoc a odpovědnost

2.1.1 *Předseda představenstva a.s., osoba jednající za společnost*

Je ze své funkce oprávněn zpracovávat osobní údaje všech fyzických osob, se kterými Správce přijde do styku v rozsahu nezbytném pro výkon své funkce. Předseda představenstva a.s. je oprávněn kontrolovat dodržování této směrnice. Je ze své funkce oprávněn zpracovávat osobní údaje uchazečů o zaměstnání a osobní údaje zaměstnanců v rozsahu nezbytném pro veškerou personální agendu. Odpovídá za aktualizaci této interní směrnice a průběžná proškolení zaměstnanců.

2.1.2 *Ostatní zaměstnanci/osoby, na které se tato směrnice vztahuje*

Jsou oprávněni zpracovávat osobní údaje v omezeném rozsahu nezbytném pro výkon své funkce.

3. Rozsah zpracovávaných osobních údajů

3.1 Rozsah zpracovávaných osobních údajů je upraven v jednotlivých záznamech o činnostech zpracování osobních údajů.

4. Ukládání, likvidace a zabezpečení osobních údajů

4.1 Ukládání, likvidace a zabezpečení osobních údajů jsou upraveny v jednotlivých záznamech o činnostech zpracování osobních údajů. Likvidace dokumentů probíhá podle spisového a skartačního řádu Správce.

5. Pověřenec pro ochranu osobních údajů

5.1 Správce není povinen mít pověřence pro ochranu osobních údajů (dále jen „pověřenec“).

6. Práva zaměstnanců

6.1 Zaměstnanec bere na vědomí, že jako subjekt údajů má následující práva:

6.2 požadovat přístup k osobním údajům týkajících se jeho osoby, jejich opravu nebo výmaz, popř. může požadovat omezení zpracování svých osobních údajů, vznášet námitky proti zpracování osobních údajů, jakož i práva na přenositelnost údajů.

6.3 požadovat, aby Správce omezil zpracování jeho osobních údajů, pokud (i) popírá přesnost svých osobních údajů, a to na dobu potřebnou k tomu, aby Správce ověřil přesnost jeho osobních údajů; (ii) zpracování jeho osobních údajů bylo protiprávní, ale nepožádá o výmaz osobních údajů, ale o omezení jejich použití; (iii) Správce již nepotřebuje jeho osobní údaje pro účely zpracování, ale zaměstnanec je požaduje pro určení, výkon nebo obhajobu svých nároků; nebo (iv) zaměstnanec vznesl námitku proti zpracování svých osobních údajů, a to do doby než bude ověřeno, zda oprávněné důvody Správce převažují nad oprávněnými důvody zaměstnance. Pokud bylo omezeno zpracování osobních údajů zaměstnance, mohou být jeho údaje zpracovány, s výjimkou uložení, pouze s jeho souhlasem.

6.4 Zaměstnanec má právo podat stížnost u dozorového orgánu, kterým je Úřad pro ochranu osobních údajů.

6.5 Zaměstnanec má právo získat od Správce kdykoliv potvrzení, že jeho osobní údaje jsou zpracovávány, a pokud tomu tak je, je Správce povinen mu na žádost poskytnout následující informace a vydat mu o nich kopii zpracovávaných osobních údajích: (i) účel zpracování; (ii) kategorie osobních údajů, které zpracovává, (iii) příjemci nebo kategorie příjemců, kterým jeho osobní údaje byly nebo budou zpřístupněny; (iv) plánovaná doba, po kterou budou jeho osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby; (v) existence práva požadovat od Správce opravu nebo výmaz osobních údajů týkajících se zaměstnance nebo omezení jejich zpracování a vznést námitku proti tomuto zpracování; (vi) právo podat stížnost u dozorového úřadu; (vii) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

6.6 Zaměstnanec má právo získat své osobní údaje, které Správce zpracovává, ve strukturovaném, běžně používaném a strojově čitelném formátu, a tyto předat jinému správci osobních údajů, pokud (i) je zpracování osobních údajů zaměstnance založeno na souhlasu se zpracováním osobních údajů; nebo (ii) zpracování se provádí automatizovaně. Pokud je to možné, předá Správce osobní údaje zaměstnance jinému správci.

6.7 Pokud zaměstnanec žádá o výkon práva podle tohoto článku, je příslušným pracovníkem pro vyřízení žádostí předseda představenstva a.s. Správce – společnosti Artlingua. Lhůta pro vyřízení požadavku je jeden měsíc od doručení žádosti a ve výjimečných případech ji lze prodloužit až o dva měsíce. Žádost o výkon práva podle tohoto článku není správním řízením ve smyslu správního řádu.

7. Realizace výkonu práv ostatních subjektů údajů

7.1 Stejná práva jako zaměstnanci mají všechny subjekty údajů. V případě požadavku na realizaci některého z práv uvedených v čl. 6 této směrnice, zejm. práva na přístup, opravu, omezení či výmaz je postup realizace práv subjektu údajů následující:

1. Požadavek na výkon práva podle GDPR je doručen Správci
2. Předseda představenstva a.s. prověří náležitosti žádosti, zejm. zda existují pochybnosti o totožnosti žadatele, případně prověří totožnost žadatele.
3. Pokud je to nutné, vyžádá si předseda představenstva a.s. relevantní informace od ostatních zaměstnanců.
4. Tito zaměstnanci poskytnou informace a podklady nutné k vyřízení žádosti.
5. Předseda představenstva a.s., resp. jiný zaměstnanec, sdělí subjektu údajů bezodkladně, nejpozději do jednoho měsíce od obdržení žádosti, jaká opatření provedl. Tuto lhůtu je možné v případě potřeby ve výjimečných případech prodloužit o další dva měsíce.

8. Zásady bezpečnosti práce s osobními údaji

8.1 Zaměstnanci jsou oprávněni používat ICT pouze k plnění svých pracovních povinností v souladu s účelem, ke kterému byly určeny.

8.2 Každý zaměstnanec se přihlašuje do počítače pod svým přihlašovacím jménem a svým heslem.

8.3 Zaměstnanci nejsou oprávněni sami instalovat, aktualizovat či opravovat počítačové programy bez souhlasu správce sítě. Všechny podstatné změny v nastavení softwaru provádí informatik.

8.4 Zaměstnanci, kteří využívají služební telefony, nesmí provádět instalaci softwarových řešení, zejm. aplikací „zdarma“. Zaměstnanci, kteří využívají služební telefony, je nesmí „půjčovat“ třetím osobám, zejm. dětem.

8.5 Pokud jsou zaměstnanci oprávněni odnášet si práci „domů“, např. na přenositelných discích, musí být tyto technologie chráněny. Nelze ukládat a odnášet mimo pracoviště dokumenty uložené např. na nezašifrovaných/nezaheslovaných flashdiscích.

8.6 Zaměstnanci jsou povinni při odchodu z pracoviště (např. pauza na oběd) odhlásit se (např. klávesová zkratka Win+L), počítač zamknout nebo vypnout. Při odchodu z pracoviště je vždy nutné počítač vypnout.

8.7 Při každém opuštění kanceláře (i na pět minut) je nutné kancelář uzamknout. Nikdy nenechávat prostor, kde je možné získat citlivá data, bez zabezpečení.

8.8 Zaměstnanci, kteří k přístupu do počítače využívají uživatelské jméno a heslo, jsou povinni nastavit heslo, že jednoduše nelze dojít k jeho prolomení a tedy, že účinně brání případným útokům. Je zakázáno používat hesla shodná s přihlašovacím jménem, biografickými údaji (např. datum narození) apod.

8.9 Zaměstnancům je zakázáno otevírat podezřelé odkazy nebo přílohy e-mailů. V případě nejasnosti jsou povinni kontaktovat informatika.

8.10 Zaměstnancům je zakázáno používat pracovní e-mail k soukromým účelům.

8.11 Při odchodu z pracoviště je nutné, aby veškeré dokumenty obsahující osobní údaje byly uklizené v prostorech k tomu určených, např. ceníky, překlady, rozpracované dokumenty, tím pádem veškerou agendu obsahující osobní údaje, včetně firemních citlivých údajů. Zaměstnanci jsou povinni zachovávat pravidlo čistého stolu.

8.12 Dokumenty obsahující citlivé osobní údaje musí být při odchodu z pracoviště uzamčeny v uzamykatelných skříňkách.

8.13 Zaměstnanci zamezí tomu, aby neoprávněné osoby měly přístup k osobním údajům. Zaměstnancům je zakázáno zejm. nechávat třetí osoby samotné v kancelářích či jiných místnostech nebo nechávat ve volně přístupné dokumenty obsahující osobní údaje bez dozoru.

8.14 Na viditelných a přístupných místech a plochách, jako jsou nástěnky apod. nesmí být vystaveny osobní a citlivé údaje.

9. Zásady zveřejňování osobních údajů na webových stránkách Správce a v místním tisku

9.1 Při přípravě článků dbají zaměstnanci na ochranu soukromí fyzických osob a poměřují zájem na zveřejnění osobních údajů dotyčných osob s právem na soukromí dotyčných osob. V případě, že právo na soukromí/ochranu osobních údajů převáží, jsou povinni si před zveřejněním obstarat souhlas dotčených osob.

9.2 *Veřejně známé osoby*

Pokud se jedná o osobu veřejně známou, např. zastupitel města, koncertující zpěvák, lze uvést jeho jméno, fotografii a profesní názory zpravidla bez dalšího. V případě, že tato

osoba sama poskytuje rozhovor místnímu tisku, např. školní časopis, není nutné žádat tuto osobu o souhlas se zveřejněním údajů, co během rozhovoru poskytla.

9.3 *Ostatní fyzické osoby – soukromé osoby*

O jiných osobách je možné zveřejňovat jejich osobní údaje zpravidla pouze s jejich souhlasem až na výjimky, které jsou uvedeny níže.

9.4 *Zveřejňování fotografií*

Zveřejňování fotografií z akcí Správce bez uvedení dalších identifikačních údajů osoby za účelem informování o činnosti Správce je možné bez souhlasu dotčené osoby, pokud fotografie necílí na zveřejnění citlivých osobních údajů nebo nemá dehonestující charakter. Ke zveřejnění fotografie se jménem je třeba souhlasu se zpracováním osobních údajů.

9.5 Citlivé osobní údaje

Zveřejnit citlivé osobní údaje bez výslovného souhlasu lze pouze ve výjimečných případech, pokud je to absolutně nezbytné pro splnění účelu zpracování. Zaměstnancům se důrazně doporučuje, aby v případě nejasnosti, zda lze údaje zveřejnit, konzultovali pověřence pro ochranu osobních údajů.

9.6 Souhlas se zpracováním osobních údajů

V případě, že nelze osobní údaje zveřejnit bez souhlasu, je pověřený pracovník povinen si souhlas dotčené osoby opatřit, jinak nesmí fotografii zveřejnit.

10. Další povinnosti zaměstnanců

10.1 Všichni zaměstnanci mají povinnost zachovávat mlčenlivost o všech osobních údajích, se kterými přijdou v rámci své činnosti pro zaměstnavatele do styku.

11. Posouzení vlivu na ochranu osobních údajů

11.1 Zavedení každého nového procesu na Správce (zejm. dotýká-li se citlivých osobních údajů), které může mít dopad na ochranu osobních údajů fyzických osob, musí příslušný zaměstnanec konzultovat s předsedou představenstva a.s.

11.2 Předseda představenstva a.s. je povinen vyhodnotit, zda nový proces podléhá povinnosti vypracovat posouzení vlivu na ochranu osobních údajů. Pokud dané zpracování osobních údajů povinnosti provést posouzení vlivu na ochranu osobních údajů

podléhá, zpracuje jej předseda představenstva a.s. ve spolupráci s příslušným zaměstnancem, a pokud je to nutné, konzultuje prostřednictvím pověřence ÚOOÚ.

11.3 I v případě, že daný proces nepodléhá posouzení vlivu na ochranu osobních údajů, je předseda představenstva a.s. nebo jiný pověřený pracovník povinen o něm zpracovat záznam o činnostech zpracování osobních údajů.

12. Hlášení porušení zabezpečení

12.1 V případě, že dojde k jakémukoliv porušení zabezpečení, je zaměstnanec povinen toto porušení nahlásit okamžitě předsedovi představenstva a.s., a pokud to není možné, pak jeho zástupci, nejpozději však do 24 hodin, co se o tomto porušení dozvěděl. Porušení zabezpečení může představovat např. ztráta flash disku, zavirovaný notebook či zneužití dat zaměstnancem.

12.2 Předseda představenstva poté, co se o porušení dozvěděl, vyhodnotí, zda došlo k porušení zabezpečení osobních údajů, zda toto porušení představuje riziko pro práva a svobody dotčených osob a zda je toto riziko vysoké. Předseda představenstva a.s. je povinen vést evidenci porušení zabezpečení osobních údajů včetně způsobu řešení dané situace a následných přijatých opatření.

12.3 Pokud předseda představenstva a.s. vyhodnotí, že porušení představuje riziko pro práva a svobody osob, je Správce povinen toto porušení bezodkladně nahlásit ÚOOÚ. Pokud od momentu porušení zabezpečení osobních údajů do momentu ohlášení ÚOOÚ uplynulo více než 72 hodin, je Správce povinen toto zdržení zdůvodnit. Toto hlášení porušení je možné provést též prostřednictvím pověřence.

12.4 Pokud předseda představenstva a.s. vyhodnotí, že porušení představuje vysoké riziko pro práva a svobody dotčených osob, je povinen o tomto porušení dále informovat postižené subjekty údajů, je-li to možné.

12.5 Všichni zaměstnanci jsou povinni předsedovi představenstva a.s. poskytnout součinnost při zjišťování a vyhodnocování porušení zabezpečení ochrany osobních údajů.

12.6 Po řešení každého porušení zabezpečení osobních údajů příslušný zaměstnanec zváží a případně navrhne předsedovi představenstva a.s., zda šlo porušení zabránit přijetím vhodných opatření, a pokud ano, zda a kdy budou tato opatření přijata.

12.7 Informatik pravidelně, nejméně však jednou za 2 měsíce, provádí kontrolu bezpečnosti systému a prověřuje, zda systém nebyl terčem útoků.

12.8 Každý zaměstnanec je v jakékoliv fázi porušení zabezpečení oprávněn konzultovat porušení zabezpečení s předsedou představenstva a.s.

13. Kontrolní činnost

13.1 Kontrolu nad dodržováním této směrnice vykonává předseda představenstva a.s.

13.2 Předseda představenstva a.s. je povinen při nástupu nového zaměstnance tohoto zaměstnance proškolit v rozsahu této směrnice.

13.3 Předseda představenstva a.s. organizuje minimálně jednou ročně průběžná školení týkající se ochrany osobních údajů. Tato školení se konají zpravidla společně s proškolením BOZP.

13.4 Porušení povinností z této směrnice, zejm. neohlášení porušení zabezpečení osobních údajů podle čl. 12 může představovat závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci, pro které je zaměstnavatel oprávněn rozvázat pracovní poměr se zaměstnancem výpovědí.

13.5 Pokud zaměstnanec poruší povinnosti z této směrnice, odpovídá zaměstnavateli za škodu podle pracovněprávních předpisů.

14. Závěrečná ustanovení

14.1 Tato směrnice nabývá účinnosti dne 25. 5. 2018