VNITŘNÍ PŘEDPIS ZAMĚSTNAVATELE
č. 1/2018

ze dne 1. 9. 2018

společnosti
EP Global Commerce a.s.
se sídlem Pařížská 130/26, Josefov, 110 00 Praha 1
IČO: 05006350
(dále jen „společnost“)

Článek 1
Účel interní směrnice a její závaznost

1.1 Tímto vnitřním předpisem se stanoví pravidla pro zpracování osobních údajů v rámci podnikatelské činnosti společnosti a nakládání s osobními údaji v souladu s obecně závaznými předpisy, kterými jsou ke dni vydání tohoto vnitřního předpisu především zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon“) a nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „nařízení“).

1.2 Tento vnitřní předpis je závazný pro všechny zaměstnance a další spolupracovníky společnosti, jak jsou definováni v čl. 2 písm. g) a j) této směrnice.

Článek 2
Definice

2.1 Pro účely tohoto vnitřního předpisu se rozumí:

a) **osobním údajem** - jakákoliv informace, která sama o sobě nebo s jinou informací může vést přímo nebo nepřímo k identifikaci subjektu údajů. Osobním údajem je např. jméno a příjmení, jsou-li uvedena společně s adresou. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřeně množství času, úsilí nebo materiálních prostředků.

b) **citlivým údajem** nebo také **zvláštním údajem** – osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu subjektu údajů, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

c) **subjektem údajů** - fyzická osoba, k níž se osobní údaje vztahují.

d) **zpracováním osobních údajů** - jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými

prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

e) správcem - každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud platné právní předpisy nestanoví jinak.

f) zpracovatelem - subjekt, který zpracovává osobní údaje pro správce a dle pokynů správce

g) zaměstnancem – 1) zaměstnanci, 2) osoby konající práci na základě dohod mimo pracovní poměr, 3) členové orgánů společnosti a 4) stážisté

h) uchazečem o zaměstnání – 1) uchazeči o zaměstnání, 2) uchazeči o výkon funkce člena společnosti a 3) uchazeči o stáž

i) obchodním partnerem – fyzická osoba, která uzavřela ze společností smlouvu, na jejímž podkladě dochází k poskytování služeb ze strany společnosti či ze strany obchodního partnera.

j) spolupracovníkem společnosti – osoby činné pro společnost na základě jiné než pracovní nebo obdobné smlouvy

k) CPO – chief protection officer, pracovník pověřený ochranou osobních údajů

Článek 3
Subjekty osobních údajů

3.1 Společnost zpracovává osobní údaje níže uvedených subjektů údajů:

a) uchazečů o zaměstnání,
b) zaměstnanců,
c) akcionářů společnosti – fyzických osob,
d) spolupracovníků společnosti,
e) obchodních partnerů společnosti, kteří jsou osobami samostatně činnými, jejich zaměstnanců a spolupracovníků,
f) osob se zájmem o spolupráci se společností.

3.2 Zpracování osobních údajů subjektů se řídí zásadami uvedenými v článku 4 této směrnice.

Článek 4
Zásady zpracování osobních údajů

4.1 Při zpracování osobních údajů je nutno důsledně dodržovat zásady obsažené v tomto článku. Nedodržení těchto zásad má za následek porušení povinností plynoucích ze zákona o ochraně osobních údajů a nařízení.

4.2 Každé zpracování osobních údajů musí mít vymezen svůj účel a musí být opřeno o některý z právních titulů uvedených v článku 5.1 této směrnice. Podrobnosti stanoví článek 5 této směrnice.

4.3 Subjekt údajů musí být vždy ještě před zahájením samotného zpracování osobních údajů informován o podmínkách, za nichž toto zpracování probíhá. K tomuto účelu slouží informační memoranda. Podrobnosti stanoví článek 7 směrnice.

4.4 Osobní údaje mohou být zpracovávány pouze v rozsahu nezbytném pro vymezený účel, a po nezbytně nutnou dobu. V případě identifikace nadbytečných či již nepotřebných osobních údajů je třeba ukončit jejich zpracování a přistoupit k jejich likvidaci. Podrobnosti stanoví článek 9 této směrnice

4.5 Je třeba přijmout a důsledně dodržovat opatření k technickému a organizačnímu zabezpečení osobních údajů. Podrobnosti stanoví článek 8 této směrnice. Pověří-li společnost zpracováním osobních údajů třetí osobu (zpracovatele), činí tak vždy na základě písemné smlouvy, v níž jsou specifikována technická a organizační opatření, jež je zpracovatel k ochraně osobních údajů povinen přijmout. V případě nedodržení těchto opatření nebo jejich selhání, je třeba postupovat v souladu s čl. 10 této směrnice.

Článek 5
Právní tituly a účely zpracování

5.1 Společnost zpracovává osobní údaje na základě těchto právních titulů:

a) plnění povinností vyplývajících z právních předpisů,
b) plnění smlouvy,
c) oprávněného zájmu společnosti,
d) souhlasu subjektu údajů.

5.2 Seznam účelů zpracování a k nim přináležejících právních titulů je obsažen v informačních memorandech, jež tvoří přílohu a nedílnou součást této směrnice.

5.3 Je-li právním titulem pro zpracování osobních údajů oprávněný zájem společnosti, musí být před zahájením zpracování provedeno posouzení, zda tento zájem převažuje nad zájmem subjektu údajů na ochraně jejich osobních údajů (balanční test). Posouzení se provede písemnou formou a výstup z tohoto posouzení je uložen u CPO. Při provádění testu se v podrobnostech postupuje dle metodiky pro balanční testy.

5.4 Je-li zpracování osobních údajů založeno na souhlasu subjektu údajů, je tato skutečnost zaznamenána v registru souhlasů vedeném CPO. Při sběru souhlasů se postupuje dle metodiky pro sběr souhlasů.

Článek 6
Informační memorandum

6.1 Informační memoranda pro jednotlivé kategorie subjektů údajů tvoří přílohu a nedílnou součást této směrnice. Jedná se o dokumenty, jejichž účelem je informovat subjekty údajů o podmínkách, za nichž dochází ke zpracování jejich osobních údajů.

6.2 Informační memoranda jsou dostupná v elektronické podobě na internetových stránkách společnosti a jsou rovněž k dispozici v listinné podobě na recepci v sídle společnosti a na personálním oddělení společnosti.

6.3 Informační memorandum může být subjektu údajů před zahájením zpracování osobních údajů fyzicky předáno (např. jako příloha smlouvy) nebo mu může být zprostředkován odkaz na ně.

Článek 7
Výkon práv subjektu údajů

7.1 Subjekt údajů má následující práva, jejichž výkon realizuje prostřednictvím společnosti jakožto správce:

a) právo na informace o zpracování osobních údajů (řešeno formou informačního memoranda – viz článek 6 této směrnice)
b) právo na přístup k osobním údajům, tzn. právo získat od společnosti potvrzení o tom, jaké jeho osobní údaje jsou zpracovávány a za jakých podmínek a právo získat kopii těchto osobních údajů
c) právo na opravu osobních údajů
d) právo na výmaz osobních údajů
e) právo na omezení zpracování osobních
f) právo na přenositelnost osobních údajů
g) právo vznést námitku proti zpracování
h) právo kdykoliv odvolat souhlas se zpracováním osobních údajů

7.2 Společnost je povinna přijmout žádosti subjektů údajů o přístup k osobním údajům všemi komunikačními prostředky za předpokladu, že bude dostatečně ověřena totožnost žadatele. V případě výkonu práva dle čl. 7.1. písm. h) této směrnice však nesmí být odvolání souhlasu komplikovanější než jeho udělení.

7.3 Všichni zaměstnanci jsou povinni zajistit, aby byly přijaté žádosti předány CPO. CPO zaznamená přijatou žádost v registru žádostí.

7.4 Žádost subjektu osobních údajů musí být vyřízena co nejdříve, nejpozději pak do jednoho měsíce od doručení žádosti. Ve výjimečných případech je možno, s ohledem na její složitost předmětem prodloužení lhůty.

7.5 Podrobnosti pro přijímání žádostí a pro jejich vyřizování stanoví metodika výkonu práv subjektů.

Článek 8
Organizační a technická opatření k ochraně osobních údajů

8.1 Společnost je povinna přijmout a udržovat organizační a technická opatření k ochraně osobních údajů. Tento článek stanoví povahu a rozsah těchto opatření.

8.2 Sídlo společnosti nachází v objektu zabezpečeném elektronickou ochranou, která je napojena na nepřetržitou službu bezpečnostní agentury. Vstup do vnitřních prostor sídla společnosti je uzamykatelný, zabezpečen vstupním čipem a kontrolován kamerou.

8.3 Přístupové klíče a vstupní čip smí být předány pouze zaměstnancům v pracovním poměru a vybraným spolupracovníkům společnosti. V případě ztráty klíče nebo čipu neoprávněné osobě musí být zámek ihned vyměněn, resp. přístupový čip zablokován.

8.4 Při ukončení pracovního poměru zaměstnance nebo jiného smluvního vztahu spolupracovníka společnosti musí být vstupní klíč a/nebo přístupový čip ihned vrácen.

8.5 Vstup třetích osob do vnitřních prostor sídla společnosti nebo jejích poboček je umožněn pouze za přítomnosti zaměstnanců nebo spolupracovníků společnosti. Třetí osoby se musí hlásit na recepci společnosti. Osamocený pohyb třetích osob ve vnitřních prostorách společnosti je zakázán.

8.6 Osobní údaje zpracovávané v listinné podobě jsou uchovávány v uzamykatelných místnostech či v trezorech, uzamykatelných šuplících a skříních.

8.7 Osobní údaje zpracovávané v elektronické podobě probíhá na serverech, na nichž je pravidelně a standardně prováděno zálohování dat. Servery společnosti jsou umístěny v:

a) sídle společnosti (tzv. serverovna);
b) zabezpečených prostorách u externího IT-dodavatele.

8.8 Informační systém společnosti je chráněn před neoprávněným přístupem zvenčí, a to zejména pomocí odpovídající brány firewall, detekce narušení, antivirového systému a podobných metod. Přístup přes bránu firewall je pravidelně kontrolován.

8.9 Pro dálkový přístup zaměstnanců a spolupracovníků společnosti z jejich mobilních zařízení/notebooků je využívána technologie VPN.

8.10 K osobním údajům mají přístup pouze osoby, jež společnost pověřila jejich zpracováním. Přístup do informačního systému společnosti je chráněn individuálním heslem zaměstnance nebo spolupracovníka. V případě ukončení pracovního nebo jiného smluvního vztahu je povinností pracovníka IT-oddělení zajistit okamžité zrušení přístupu zaměstnance či spolupracovníka.

8.11 Zaměstnanci a spolupracovníci společnosti jsou povinni udržovat svá hesla v tajnosti a neumožnit třetí osobě seznámení se s heslem. V případě, že se s heslem seznámí třetí osoba, jsou zaměstnanci nebo spolupracovníci povinni neprodleně zajistit změnu hesla a oznámit tuto skutečnost pracovníkovi IT-oddělení.

8.12 Vstupovat do informačního systému společnosti pod cizím heslem se zakazuje. To neplatí, byl-li pracovní nebo smluvní vztah zaměstnance nebo spolupracovníka ke společnosti ukončen a nelze-li plnění pracovních úkolů společnosti zajistit jinak.

8.13 Za správu hesel a přístupových práv odpovídá pracovník IT-oddělení a externí dodavatel IT služeb.

8.14 Osobní údaje smí být kopírovány pouze z důvodu plnění pracovních úkolů a pouze v nezbytném rozsahu. Kopírování osobních údajů v elektronické podobě na pevný disk jednotlivých počítačů nebo na jiný nosič dat je povoleno pouze podmínky, že přístup k těmto údajům je blokován přístupovým heslem konkrétního zaměstnance nebo spolupracovníka.

8.15 Osobní údaje v papírové formě se mimo společnost předávají osobně, prostřednictvím pošty nebo kurýra. Při poskytování osobních údajů prostřednictvím elektronické pošty jsou e-maily enkryptovány.

8.16 Osobní údaje mohou být zpracovávány také mimo prostory společnosti. Mimo prostory společnosti zpracovávají osobní údaje zaměstnanci a spolupracovníci společnosti, kterým byl umožněn home-office a/nebo kteří disponují elektronickým zařízením s dálkovým přístupem. Zaměstnanec nebo spolupracovník disponující osobními údaji mimo sídlo společnosti nebo její pobočky je odpovědný za jejich ochranu před neoprávněným zásahem.

8.17 Zaměstnanci jsou oprávněni používat pro svou osobní potřebu výrobní a pracovní prostředky společnosti včetně výpočetní techniky a telekomunikačního zařízení. Zaměstnanci jsou povinni i v tomto případě dodržovat všechna bezpečností opatření při používání výrobních a pracovních prostředků společnosti, zejména co se týče šifrování, užívání uživatelských účtů a používání hesel a zacházení s nimi.

8.18 Zaměstnanci a spolupracovníci společnosti jsou povinni zachovávat přísnou mlčenlivost o zpracovávaných údajích i o bezpečnostních opatřeních přijatých společností k jejich ochraně. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného smluvního vztahu.

8.19 Zaměstnanci a spolupracovníci společnosti jsou v pravidelných intervalech (nejméně jednou za dva roky) školeni v oblasti ochrany osobních údajů a jsou seznamováni s novými opatřeními v této oblasti.

Článek 9
Archivace a likvidace osobních údajů

9.1 Společnost je povinna archivovat osobní údaje podle druhu dokumentu, v němž jsou uvedeny. Archivační lhůty jednotlivých dokumentů jsou uvedeny ve spisovém a skartačním řádu společnosti.

9.2 Zaměstnanci a spolupracovníci společnosti jsou povinni likvidovat osobní údaje, ihned jakmile pomine důvod pro jejich zpracování.

9.3 Listiny osahující osobní údaje jsou likvidovány prostřednictvím skartovacích strojů nebo externí skartovací firmy.

9.4 Likvidace osobních údajů v elektronické podobě se provede úplným vymazáním údajů ze serveru, ze zálohového disku nebo jiného nosiče.

Článek 10
Bezpečnostní incidenty a způsob jejich řešení

10.1 Bezpečnostní incident je jakákoliv událost, jež je způsobilá ohrozit bezpečnost, důvěrnost, dostupnost nebo integritu osobních údajů. Bezpečnostní incident může spočívat v nedodržení pravidel pro ochranu osobních údajů stanovených v článku 8 této směrnice, nebo v jiné událostí, jejímž následkem je ztráta osobních údajů, jejich neoprávněné použití či zpřístupnění.

10.2 Zaměstnanci a spolupracovníci společnosti jsou povinni každý bezpečnostní incident, o kterém se dozví a který ještě nebyl nahlášen, bezodkladně oznámit svému nadřízenému pracovníkovi a CPO. CPO následně posoudí, zda je pravděpodobné, že dané porušení zabezpečení osobních údajů má za následek riziko pro práva a svobody fyzických osob. Pokud ano, je nezbytné bezpečnostní incident bez zbytečného odkladu (nejpozději však do 72 hodin) ohlásit příslušnému dozorovému úřadu a v případě, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzické osoby, rovněž dotčeným subjektům údajů.

10.3 Při posuzování rizika pro práva a svobody fyzických osob se vychází zejména z kategorie osobních údajů, které byly porušením zabezpečení dotčeny (zejména jedná-li se o citlivé údaje), povaze bezpečnostního incidentu a počtu dotčených subjektů údajů.

10.4 Všechny bezpečnostní incidenty jsou evidovány ve zvláštním registru, spravovaném CPO, a to bez ohledu na to, zda bylo nutno incident hlásit dozorovému úřadu či nikoliv.

10.5 Podrobnější úprava je obsažena v metodice hlášení bezpečnostních incidentů.

Článek 11
Záznamy o činnostech zpracování

11.1 Společnost vede za účelem dokladování souladu s nařízením záznamy o činnostech zpracování osobních údajů.

11.2 Záznamy o činnostech zpracování jsou vedeny v elektronické podobě. Za řádné vedení těchto záznamů odpovídá CPO.

11.3 Záznamy o činnostech zpracování obsahují nejméně následující informace:

a) identifikační údaje správce
b) výčet účelů zpracování
c) popis kategorií subjektů údajů a osobních údajů
d) výčet kategorií příjemců osobních údajů, kterým osobní údaje budou nebo byly zpřístupněny;
e) údaj o tom, zda dochází k předání osobních údajů do třetí země (mezinárodní organizaci) a pokud ano, do které
f) údaj o plánované době zpracování (lhůty pro výmaz)

g) popis organizačních a technických opatření přijatých k ochraně osobních údajů (je-li to možné).

Článek 12
Pracovník pověřený ochranou osobních údajů (CPO)

12.1 Společnost pověří úkoly v oblasti ochrany osobních údajů konkrétní osobu či osoby (CPO).

12.2 Pracovník pověřený ochranou osobních údajů (CPO)

a) je kontaktní osobou pro všechny subjekty údajů,
b) dohlíží na dodržování zásad zpracování osobních údajů,
c) monitoruje dodržování technických a organizačních opatření k zajištění bezpečnosti osobních údajů, upozorňuje na nedostatky a navrhuje opatření ke zlepšení ochrany osobních údajů,
d) odpovídá na žádosti subjektů údajů ohledně výkonu jejich práv, vede registr žádostí,
e) vede registr souhlasů se zpracováním osobních údajů,
f) vede záznamy o činnostech zpracování,
g) vede evidenci bezpečnostních incidentů a vyhodnocuje jejich povahu.

Článek 13
Závěrečná ustanovení

13.1 Stávající zaměstnanci společnosti a její spolupracovníci byli s tímto vnitřním předpisem ke dni jeho vyhlášení seznámeni. Každý nový zaměstnanec a spolupracovník musí být s tímto vnitřním předpisem seznámen před nástupem do práce, resp. zahájením spolupráce.

13.2 Tento vnitřní předpis se vydává na dobu neurčitou, bude však v pravidelných intervalech aktualizován.

13.3 Tento vnitřní předpis nabývá platnosti a účinnosti dnem vyhlášení. Tímto vnitřním předpisem se ruší a zcela nahrazuje veškeré předchozí směrnice a opatření v oblasti ochrany osobních údajů ve společnosti.