Vnitřní směrnice č. 01-18– Zpracování osobních údajů

(dále jen „směrnice“)

EUFRAT Group, s. r. o.

IČO: 27961281

se sídlem Plzeň - Východní předměstí, Pallova 42/8, PSČ 30112

zapsaná v obchodním rejstříku vedeném Krajským soudem v Plzni, oddíl C, vložka 18780

zastoupená Bc. Danuší Burešovou, jednatelkou

(dále jen „**společnost**“)

I. Obecná ustanovení

1. Společnost tímto na základě ustanovení § 305 zákona č. 262/2006 Sb., zákoníku práce, v platném znění, vydává tuto vnitřní směrnici č. 01-18, kterou se upravují postupy, podmínky a způsoby zpracování osobních údajů fyzických osob zaměstnanci 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 (dále jen „**GDPR**“).
2. Touto směrnicí jsou povinni se řídit zaměstnanci společnosti a v přiměřeném rozsahu také členové orgánů společnosti, společníci a jiné osoby podílející se na chodu společnosti.
3. Společnost je správcem ve smyslu ust. článku 4 odst. 7 GDPR.

II. Základní pojmy

1. „**Osobními údaji**“ se rozumí 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;
2. „**Zpracováním**“ se rozumí 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. „**Správcem**“ je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Evropské unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Společnost EUFRAT Group, s.r.o. je správcem ve smyslu tohoto odstavce a ve smyslu ust. článku 4 odst. 7 GDPR;

4. „**Zpracovatelem**“ je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
5. „**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;
6. „**Porušením zabezpečení osobních údajů**“ se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
7. „**Dozorovým úřadem**“ se rozumí Úřad pro ochranu osobních údajů, IČO: 70837627, sídlem Pplk. Sochora 27, 170 00, Praha 7.

III. Základní zásady

1. V tomto článku III. jsou níže uvedeny základní zásady, kterými jsou zaměstnanci povinni se při zpracování osobních údajů fyzický osob řídit.
2. **Zásada zákonnosti, korektnosti a transparentnosti** – osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem;
3. **Zásada účelového omezení** – osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 GDPR nepovažuje za neslučitelné s původními účely;
4. **Zásada minimalizace údajů** - osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány;
5. **Zásada přesnosti** – osobní údaje musí být 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;
6. **Zásada omezení uložení** – osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů;
7. **Zásada integrity a důvěrnosti** – osobní údaje musí být 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
8. Společnost nejmenovala pověřence pro ochranu osobních údajů ve smyslu ust. čl. 37 a násl. GDPR. Osobou pověřenou pro styk s osobními údaji je Bc. Danuše Burešová, +420 602 491 861, dana.buresova@eufrat.cz (dále „**pověřená osoba**“). V případě dotazů

týkajících se zpracovávání osobních údajů a dodržování pravidel a povinností dle této směrnice se mohou zaměstnanci obrátit na svého nadřízeného nebo pověřenou osobu.

IV. Zpracovávané osobní údaje

1. Společnost zpracovává tyto osobní údaje o zaměstnancích v pracovněprávním vztahu ke společnosti/členech orgánů společnosti a bývalých zaměstnancích/členech orgánů společnosti: jméno, příjmení, adresa trvalého bydliště, doručovací adresa, číslo bankovního účtu, datum narození, rodné číslo, zdravotní pojišťovnu, vzdělání, odbornou praxi, počet dětí a jejich stáří, stav (v manželství či nikoliv), telefon, e-mail, a další osobní údaje, které uchazeč předal společnosti a jejichž potřeba zpracování vyplývá z účelů, za nimiž jsou takové osobní údaje zpracovávány, a dále osobní údaje vzniklé v souvislosti s jejich pracovněprávním vztahem ke společnosti (např. údaje o pracovním výkonu, odborné a osobnostní způsobilosti, odměňování, apod.) a to vše společnost činí za účely, právními důvody a po dobu uvedenou v dokumentu „Informace o zpracování osobních údajů zaměstnanců, uchazečů o zaměstnání a členů orgánu správce“, který je přílohou této směrnice.
2. Společnost zpracovává tyto osobní údaje o společnících: jméno, příjmení, adresa trvalého bydliště, doručovací adresa, číslo bankovního účtu, datum narození, rodné číslo, telefon, e-mail, a další osobní údaje, jejichž potřeba zpracování vyplývá z účelů, za nimiž jsou takové osobní údaje zpracovávány, a to vše společnost činí za účely, právními důvody a po dobu uvedenou v dokumentu „Informace o zpracování osobních údajů společníků“, který je přílohou této směrnice.
3. Společnost zpracovává tyto osobní údaje o uchazečích o zaměstnání/výkon funkce člena orgánu společnosti: jméno, příjmení, adresa trvalého bydliště, doručovací adresa, datum narození, telefon, e-mail, vzdělání, odbornou praxi, odborná způsobilost a další osobní údaje, které uchazeč předal společnosti a jejichž potřeba zpracování vyplývá z účelů, za nimiž jsou takové osobní údaje zpracovávány, a to vše společnost činí za účely, právními důvody a po dobu uvedenou v dokumentu „Informace o zpracování osobních údajů zaměstnanců, uchazečů o zaměstnání a členů orgánu správce“, který je přílohou této směrnice.
4. Společnost zpracovává tyto osobní údaje o současných, minulých nebo potenciálních zákaznících, odběratelích, dodavatelích a smluvních partnerech (dále jen „**smluvní partner**“): jméno, příjmení, IČO, DIČ, sídlo, adresa provozovny, adresa bydliště, doručovací adresa, číslo bankovního účtu, telefon, e-mail, a další osobní údaje, které smluvní partner předal společnosti a jejichž potřeba zpracování vyplývá z účelů, za nimiž jsou takové osobní údaje zpracovávány, a dále osobní údaje vzniklé v souvislosti s jejich smluvním vztahem ke společnosti (např. údaje o objednávkách, nabídkách, dodáních, předávací protokoly, dodací listy, reklamace a jejich vyřízení apod.) a to vše společnost činí za účely, právními důvody a po dobu uvedenou v dokumentu „Informace o zpracování osobních údajů zákazníků, odběratelů, dodavatelů a smluvních partnerů“, který je přílohou této směrnice.
5. Společnost dále zpracovává osobní údaje o subjektech údajů uvedených v ust. odst. 1. až 4. tohoto článku směrnice, které zjistil z veřejně přístupných registrů (např. veřejné rejstříky právnických a fyzických osob, živnostenský rejstřík, insolvenční rejstřík, centrální evidence

exekucí) a to v rozsahu: jméno, příjmení, IČO, DIČ, sídlo, adresa provozovny, živnostenská oprávnění, vedené exekuce proti subjektu údajů, vedené insolvenční řízení subjektu údajů, výkon funkce v orgánech právnických osob.

6. Společnost zpracovává osobní údaje o fyzických osobách v postavení subjektů údajů, které byly zaznamenány kamerovým systémem provozovaný společností, v tomto rozsahu: podoba, pohyb, přítomnost, jednání a chování subjektu údajů na snímaném místě v konkrétní čas, a to vše společnost činí za účely, právními důvody a po dobu uvedenou v dokumentu „Informace o zpracování osobních údajů – kamerový systém“, který je přílohou této směrnice.

7. Zaměstnanec, který od subjektu údajů převezme jeho osobní údaje, je povinen ještě před převzetím nebo nejpozději obratem po převzetí osobních údajů subjekt údajů v souladu s ust. čl. 13 a 14 GDPR informovat o zpracovávání jeho osobních údajů společností. Zaměstnanci informují subjekt údajů dle předcházející věty prostřednictví dokumentu „Informace o zpracování osobních údajů“ (příslušného dle skupiny osob, do níž subjekt patří) nebo dokumentu „Zkrácená informace o zpracování osobních údajů“, který subjektu údajů zašlou elektronickou poštou nebo mu ho předají v listinné podobě a taktéž ho upozorní na to, že „Informace o zpracování osobních údajů“ je v průběžně aktualizované verzi volně dostupná na internetových stránkách společnosti: https://www.eufrat.cz/o-nas/ochrana-osobnich-udaju/informace-o-zpracovani-osobnich-udaju-univerzalni-obchod/. „Zkrácená informace o zpracování osobních údajů“ je zahrnuta ve vybraných obchodních materiálech – nabídky, objednávky, formuláře a jiné listiny, na základě nichž společnost získá osobní údaje subjektu údajů.

8. V případě uchazečů o zaměstnání nebo výkon funkce orgánu ve společnosti (jakož i osob, které budou uzavírat pracovní smlouvu nebo smlouvu o výkonu funkce bez výběrového řízení) jsou zaměstnanci společnosti povinni těmto osobám předložit dokument „Informace o zpracování osobních údajů“ v listinné podobě (vytištěný) k seznámení a zajistit datovaný podpis uchazeče na dokumentu, který následně musí být založen do složky vedené pro uchazeče a později případně zaměstnance/člena orgánu společnosti. Zaměstnanci společnosti jsou povinni rozlišovat a užívat druhy dokumentu „Informace o zpracování osobních údajů“ podle skupiny osob, do níž subjekt údajů patří, jak jsou tyto dokumenty uvedeny v příloze této směrnice.

9. Mimo osobních údajů zpracovávaných společností ze zákonných důvodů, jak je uvedeno výše v odst. 1. až 5. tohoto článku směrnice, zpracovává společnost také osobní údaje na základě souhlasu subjektu údajů. Přednost před zpracováváním osobních údajů na základě souhlasu má užití výše uvedených zákonných důvodů, a proto je každý zaměstnanec přebírající nebo vyžadující osobní údaje od subjektu údajů povinen zhodnotit, zda vyžadované osobní údaje a účel jejich vyžádání spadá pod některý z výše uvedených (nebo jiných dle GDPR) zákonných důvodů. Zaměstnanec si od subjektu údajů vyžádá souhlas teprve v případě, že nelze užít jiný zákonný důvod. Souhlas musí být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, nebo učiněného elektronicky (nutné ověřit totožnost osoby např. telefonicky nebo SMS). Souhlas musí být poskytnut pro všechny předpokládané účely zpracování osobních údajů a zaměstnanec nesmí uzavření smlouvy se subjektem údajů

podmiňovat udělením souhlasu – neudělení souhlasu nesmí být překážkou uzavření smlouvy (musí být zajištěna svoboda rozhodnutí subjektu údajů).

10. Společnost je povinna prokázat, že subjekt údajů udělil souhlas se zpracováním osobních údajů, a proto je nutné pečlivě uschovat veškeré vyjádřené souhlasy a tyto založit do složky vedené pro potřeby subjektu údajů. Zaměstnanec je povinen sdělit subjektu údajů veškeré účely zpracování osobních údajů, k nimž má být souhlas udělen, dobu trvání zpracování osobních údajů, údaje společnosti a způsob odvolání souhlasu. Vzor souhlasu se zpracováním osobních údajů je přílohou této směrnice. Souhlas musí být opatřen datovaným podpisem subjektu údajů (písemný souhlas se upřednostňuje), v případě elektronického souhlasu musí být tento také datován a totožnost subjektu údajů udělujícího souhlas musí být ověřena zaměstnancem.

11. V případě odvolání souhlasu subjektem údajů je zaměstnanec, u něhož bylo odvolání souhlasu uplatněno, bez zbytečného odkladu, nejpozději do skončení pracovní doby předmětného dne, informovat pověřenou osobu o odvolání souhlasu. Pověřená osoba je povinna nejpozději do 5 pracovních dnů ode dne odvolání souhlasu zajistit výmaz veškerých osobních údajů zpracovávaných společností na základě odvolaného souhlasu, a to jak v elektronické, tak v písemné formě.

12. Za obsahovou správnost, kompletnost a následné uložení dat v elektronické nebo písemné formě v okamžiku pořízení či změny zodpovídá vždy ten, kdo data pořídil či změnil bez ohledu na to, odkud byla data získána a v čí pracovní náplni je sběr a zpracovaní těchto dat.

13. Zaměstnanec, zaznamenávající osobní údaje v elektronické nebo písemné formě, je povinen vždy si řádně ověřit věrohodnost a správnost těchto údajů.

14. Zaměstnanec, který zjistí nesrovnalost mezi aktuálně zjištěným údajem a údajem zpracovávaným společností v elektronické nebo písemné formě, je povinen tuto skutečnost neprodleně ohlásit svému nadřízenému nebo pověřené osobě a spolupodílet se na zajištění nápravy.

V. Kamerový systém

1. Společnost provozuje automatizovaný kamerový systém se záznamem. Za provoz, nastavení, fungování a plnění povinností společnosti v souvislosti s ochranou osobních údajů je odpovědná pověřená osoba určená společností.

2. Kamerový systém sestává z celkem 20 ks kamer, které jsou rozmístěny na následujících místech:

BUDOVA A (centrála Plzeň, Pallova 8)
1. NP
1 před hlavním vchodem
2. NP
1 recepce
1 chodba před recepcí
1 chodba před učebnami

BUDOVA B (centrála Plzeň, Pallova 8)
1. NP

1 před hlavním vchodem
1 chodba pod schodištěm do 2. NP
1 chodba u kuchyňky
1 kuchyňka
2 prostor u kopírky
1 lektorská místnost
1 chodba před kancelářemi

2. NP

1 chodba u kuchyňky
1 učebna Tokio

BUDOVA C (centrála Plzeň, Pallova 8)

1. NP

1 1 x chodba před kanceláří

BUDOVA D (pobočka Plzeň-Černice, Vltavínová 1)

1. NP

1 prostor u kopírky
1 chodba před učebnami
1 učebna Oslo
1 učebna Stockholm
1 učebna Helsinky

3. Kamerový systém funguje nepřetržitě. Obrazové záznamy bez zvukové stopy jsou uchovávány po nezbytně nutnou dobu, a to maximálně po dobu 72 hodin, kdy jsou následně automaticky přepsány novým záznamem. Záznamy se ukládají na 3 serverech, které jsou všechny umístěny lokálně v prostorách společnosti.

4. Žádná z umístěných kamer neohrožuje důstojnost a volný pohyb osob, které se nacházejí v místě snímaném kamerou. Kamerami nejsou zásadně snímány prostory, kde by mohlo být nepřiměřeně zasahováno do soukromého a osobního života subjektů údajů, zejména sociální zařízení, šatny pro zaměstnance, jakož i další prostory, jejichž monitorování není nezbytné pro naplnění účelu zpracování osobních údajů.

5. Prostor snímaný kamerou je označen viditelným štítkem, na němž je uvedeno přinejmenším následující sdělení: *„PROSTOR JE STŘEŽEN KAMEROVÝM SYSTÉMEM SE ZÁZNAMEM.“*

6. Pouze pověřená osoba, případně osoba k tomu pověřenou osobou nebo statutárním orgánem společnosti určená je oprávněna:

a. nastavovat, ovládat a obsluhovat kamerový systém;
b. vyměňovat staré kamery za nové, zajišťovat opravu kamer;
c. přehrávat, editovat, exportovat nebo mazat nahraná data.

7. Jakékoliv zpřístupnění záznamů kamerového systémů nebo předání nahrávky kamerového systému společnost eviduje ve zvláštní evidenci.

8. O rozmístění kamer, jejich odstraňování (nikoliv výměně za novou) a umisťování nových kamer rozhoduje statutární orgán společnosti.

9. Na obsluhu a jakékoliv jiné zacházení s kamerovým systémem se přiměřeně použijí zásady, pravidla a postupy uvedené níže v článcích VI. a VII. této směrnice.

VI. Ochrana dat obsahujících osobní údaje a povinnosti zaměstnanců při práci s osobními údaji

1. Smyslem ochrany dat, jejichž předmětem jsou osobní údaje (dále též jako „**data**“), je učinit taková organizační a technická opatření, která v nejvyšší možné míře omezí možnost nenávratného poškození nebo ztráty dat, minimalizují negativní dopady způsobené poškozením nebo ztrátou dat na další činnost společnosti. Přijatá opatření zamezí přístup k datům nepovolaným osobám.
2. Předmětem ochrany je veškeré programové vybavení včetně doprovodné dokumentace, všechna provozní data uložená na nosičích informací, v operační paměti počítačů, tiskáren a dalších zařízení výpočetní techniky, záložní a archivní kopie dat uložené na nosičích informací, údaje zobrazené nebo vytištěné na výstupních zařízeních; přístupová hesla, technické informace o informačním systému a návody.
3. Všichni zaměstnanci, kteří přicházejí do styku s výpočetní technikou, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí možnou ztrátu a trvalé poškození provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, poruchou ICT (informační a komunikační technologie), požárem, živelní pohromou atp.
4. Provozní data, která jsou uložena na pevných discích počítačů, musí být zálohována v počítačové síti, popřípadě na dalších nosičích informací.
5. Osobní údaje lze uchovávat pouze na počítačích vybavených operačním systémem, který umožňuje nastavování přístupových práv k souborům.
6. Zaměstnanci jsou povinni dodržovat zejména následující pravidla ochrany dat s osobními údaji:

a. znemožnění jakéhokoli přístupu nepovolaných osob k výpočetní technice a datům, a to jak v pracovní, tak i v mimopracovní době;
b. neponechávání zapnuté techniky bez dozoru;
c. situování pracoviště tak, aby nebylo možno odečítat údaje z monitorů nepovolanými osobami;
d. uložení tiskových výstupů mimo dosah nepovolaných osob;
e. přístup k počítači (server, lokální stanice, notebook apod.), pracovnímu telefonu a tabletu musí být zabezpečen heslem, aby byl znemožněn přístup nepovolané osobě
f. přístup k adresářům a souborům s osobními údaji je řízen přístupovými právy určených osob;
g. heslo je tvořeno nejméně osmi znaky, vždy obsahuje kombinaci číslic, malých a velkých písmen, nejde o snadno odhalitelný text obsahující jména, příjmení, data narození, rodné číslo;
h. udržování všech hesel v tajnosti, častá změna hesla – alespoň 1x za 6 měsíců;
i. není dovoleno přesunovat, odpojovat, přenášet, připojovat a ani jinak manipulovat s umístěným stolním počítačem;

j. jakoukoli závadu nebo i podezření na nestandardní fungování počítače, notebooku, tabletu nebo telefonu zaměstnanec bez zbytečného odkladu hlásí svému nadřízenému nebo pověřené osobě;
k. v případě elektronické komunikace a zasílání dat včetně osobních údajů subjektů údajů jsou zaměstnanci povinni dbát o to, aby osobní údaje nebyly neodůvodněně rozesílány nepovolaným osobám, zejména je třeba obezřetně užívat v e-mailové komunikaci funkci „odpovědět všem“;
l. výslovně se zakazuje ponechávat spisy, složky a jakékoliv jiné dokumenty obsahující osobní údaje subjektů údajů bez dozoru ve vozidle (ani po jeho uzamčení, ani v případě služebního vozidla) nebo ve skříňce či jiném místě určeném veřejnosti a návštěvníkům předmětného zařízení k odkládání svršků mimo pracoviště zaměstnance (např. bazén, fit-centrum, knihovna, úschovna zavazadel).

7. Správce sítě je oprávněn v rámci své kompetence monitorovat vytížení sítě a oprávněnost využívání jednotlivými uživateli. Toto ustanovení může být využíváno pro identifikaci přestupků uživatelů v souladu s platnou právní úpravou.

8. Písemnosti a média s osobními údaji je zakázáno rozmnožovat bez souhlasu nadřízeného nebo pověřené osoby.

9. Zaměstnanci jsou při jakýchkoliv činnostech souvisejících se zpracováním osobních údajů povinni:

a. zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení pracovního poměru u společnosti
b. zajišťovat, aby nedošlo ke zcizení nebo nahodilému přístupu k osobním údajům nepovolanými osobami, ke změně, zničení či ztrátě nebo neoprávněným přenosům osobních údajů, k jinému neoprávněnému zpracování osobních údajů, jakož i k jejich jinému zneužití
c. shromažďovat a zpracovávat pouze osobní údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro jeho naplnění
d. shromažďovat a zpracovávat pouze pravdivé, přesné a ověřené údaje
e. průběžně ověřovat trvání účelu a právního důvodu a nepřekročení doby pro zpracování osobních údajů v souladu s článkem IV. této směrnice

VII. Zásady pro práci s výpočetní technikou

1. Při práci s výpočetní technikou je zakázáno:

a. používat nelegální software;
b. používat software, jehož použití nebylo schváleno správcem ICT;
c. instalovat bez svolení správce ICT na disky počítačů jakýkoliv nelegální software či data s tímto programovým vybavením související;
d. odstraňovat instalovaný software nebo provádět změny v nastavení a umístění software a souvisejících dat;
e. pořizovat kopie software a dat pro jinou než pracovní potřebu;
f. předávat data jiným subjektům bez předchozího souhlasu příslušného vedoucího pracovníka;
g. provádět demontáž, úpravy, opravy, změny v nastavení a zapojení prostředků ICT, používat prostředky ICT pro jiné než schválené účely;
h. instalovat a hrát počítačové hry.

2. Zaměstnanci jsou povinni používat a soustavně udržovat aktualizovaný antivirový program a další funkcionality operačního systému.
3. Při zahájení práce s ICT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. Ukončování činnosti programů se provádí předepsaným způsobem, včetně ukončení práce v síti. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěřené prostředky, tj. osobní počítače, tiskárny, modemy atd. vypnuty, s výjimkou těch zařízení, která musí zůstat s ohledem na své určení trvale zapnuta.
4. Při ukončení nebo změně pracovněprávního vztahu správce sítě provede úpravu uživatelského účtu zaměstnance, včetně přístupových práv.
5. Tištěné výstupy nebo jiné listinné dokumenty obsahující osobní údaje je příslušný zaměstnanec při opuštění prostoru, kde jsou tyto dokumenty uchovávány, povinen v případě nepřítomnosti jiné oprávněné, povolané nebo pověřené osoby k nakládání s osobními údaji zabezpečit před neoprávněným přístupem nepovolaných osob (např. ponecháním v uzamykatelném nábytku, uzamykatelné místnosti).

VIII. Archivace, skartace dat

1. Osobní údaje se uchovávají pouze po dobu nezbytnou k účelu jejich zpracování v souladu s článkem IV. této směrnice. Po zániku účelu a právního důvodu pro zpracování osobních údajů (uplynutí doby) jsou zaměstnanci povinni informovat svého nadřízeného o nutnosti vymazání osobních údajů v elektronické podobě a skartaci dokumentů s osobními údaji v listinné podobě. Zaměstnanec je v takovém případě povinen postupovat v souladu s vnitřním předpisem upravujícím archivaci a skartaci dokumentů.
2. Elektronická data s osobními údaji se zálohují na centrálním serveru. Pro přenos dat se ve společnosti používá síť, USB flash disky. Dokumenty s osobními údaji v listinné podobě jsou archivovány v souladu s vnitřním předpisem upravujícím archivaci a skartaci dokumentů.
3. Každý zaměstnanec je povinen provádět zálohování dat podle rozpisu zálohování. Denně jsou zálohována data v účetnictví. Týdně jsou zálohována data, ze kterých jsou vytvářeny tiskové výstupy. Zaměstnanci uchovávají data na počítači v určené složce, aby je bylo možné snadno zálohovat (nebo aby byly zálohovány automaticky). Při ukončení pracovněprávního vztahu zaměstnance bude provedeno zálohování dat vždy.
4. Zálohována jsou všechna data, nikoli programy nebo operační systém. Zálohy jsou ukládány mimo místnost, kde je počítač umístěn (aby zálohy nemohly být odcizeny nebo poškozeny spolu s počítačem, který je zálohován).
5. Správce ICT vede přehled o instalaci software na jednotlivé pracovní stanice a jeho kontrolách. Jakékoli porušení této směrnice hlásí svému vedoucímu pracovníkovi.

IX. Práva subjektů údajů

1. Níže jsou uvedena práva subjektů údajů dle ust. čl. 15 a násl. GDPR, která subjekty údajů mohou vůči společnosti jakožto správci údajů uplatnit. Zaměstnanci a zejména pověřené osoby jsou povinni se s těmito právy subjektů údajů seznámit.

2. **Právo na přístup k osobním údajům**

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

a. účely zpracování;
b. kategorie dotčených osobních údajů;
c. příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
d. plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
e. existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, nebo vznést námitku proti tomuto zpracování;
f. právo podat stížnost u dozorového úřadu;
g. veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
h. skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4 GDPR, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Společnost je povinna poskytnout kopii zpracovávaných osobních údajů subjektu údajů. Právem získat kopii zpracovávaných osobních údajů nesmějí být nepříznivě dotčena práva a svobody jiných osob.

3. **Právo na opravu**

Subjekt údajů má právo na to, aby společnost jako správce bez zbytečného odkladu opravila nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

4. **Právo na výmaz („právo být zapomenut“)**

Subjekt údajů má právo na to, aby společnost jako správce bez zbytečného odkladu vymazala osobní údaje, které se daného subjektu údajů týkají, a společnost má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a. osobní údaje 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 podle čl. 21 odst. 1 GDPR a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2 GDPR;
d. osobní údaje byly zpracovány protiprávně;
e. osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Evropské unie nebo členského státu, které se na společnost vztahuje;
f. osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1. GDPR

5. **Právo na omezení zpracování**

Subjekt údajů má právo na to, aby společnost jako správce omezila zpracování, v kterémkoli z těchto případů:

a. subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby společnost mohla přesnost osobních údajů ověřit;
b. zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho omezení jejich použití;
c. společnost 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 podle čl. 21 odst. 1 GDPR, dokud nebude ověřeno, zda oprávněné důvody společnosti převažují nad oprávněnými důvody subjektu údajů.

Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Evropské unie nebo některého členského státu. Subjekt údajů, který dosáhl omezení zpracování, je společnost povinna předem upozornit na to, že bude omezení zpracování zrušeno.

6. **Právo na přenositelnost údajů**

Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl společnosti jako správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu společnost, které byly osobní údaje poskytnuty, bránila, a to v případě, že:

a. zpracování je založeno na jeho souhlasu se zpracováním osobních údajů, a
b. zpracování se provádí automatizovaně.

Při výkonu svého práva na přenositelnost údajů má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

7. **Právo vznést námitku**

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, na základě čl. 6 odst. 1 písm. e) nebo f) GDPR, včetně profilování založeného na těchto ustanoveních. Společnost jako správce osobní údaje dále nebude zpracovávat, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

8. **Právo odvolat svůj souhlas se zpracováním osobních údajů**

Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu musí být subjekt údajů o tomto právu informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

X. Uplatňování práv subjektů údajů

1. Subjekt údajů může uplatnit svá práva uvedená článku IX. této směrnice vůči společnosti prostřednictvím formuláře „Žádost – uplatnění práv subjektu údajů“ (dále jen „**Žádost**“), která tvoří Přílohu č. 4 této směrnice. Žádost je v aktualizované verzi volně dostupná v tištěné podobě v sídle společnosti (na recepci, jejíž obsluha je povinna zajistit bezplatné vytištění formuláře Žádosti v případě takového požadavku subjektu údajů) a v elektronické podobě na webovém odkazu https://www.eufrat.cz/o-nas/ochrana-osobnich-udaju/zadost-uplatneni-prav-subjektu-udaju/
2. Za vyřízení Žádosti, její prošetření a odpověď na tuto Žádost je odpovědná pověřená osoba. Pověřená osoba je povinna pečlivě podanou Žádost přezkoumat z hlediska oprávněnosti jednotlivých práv a nároků uplatněných subjektem údajů ve srovnání s právy dle článku VIII. této směrnice a příslušnými ustanoveními GDPR. Pověřená osoba je povinna prověřit skutkové okolnosti Žádosti a osobních údajů subjektu údajů (žadatele) a vyžádat si veškeré osobní údaje evidované v elektronické a listinné podobě, včetně případné evidence provedených úkonů v rámci zpracovávání osobních údajů.
3. Pověřená osoba po provedení postupu dle odst. 2 tohoto článku sdělí svému nadřízenému odůvodněné písemné stanovisko se závěrem, zda má být Žádosti vyhověno či nikoliv, případně v jakém rozsahu, a to nejpozději do 10 kalendářních dní ode dne uplatnění Žádosti. Nadřízený pověřené osoby po přednesení stanoviska rozhodne, jakým způsobem bude Žádost vyřízena (vyhověno/nevyhověno/částečně vyhověno) a toto rozhodnutí sdělí pověřené osobě nejpozději do 5 kalendářních dnů ode dne, kdy obdržel písemné stanovisko pověřené osoby. Po obdržení rozhodnutí o způsobu vyřízení Žádosti je pověřená osoba povinna nejpozději do 5 kalendářních dnů odpovědět subjektu údajů (žadateli), jakým způsobem byla jeho Žádost vyřízena a v případě kladného vyřízení Žádosti (v rozsahu vyhovění Žádosti) je pověřená osoba povinna provést veškeré úkony tak, aby byla práva uplatněná Žádostí uspokojena. V případě nedodržení uvedených lhůt, a pakliže uplyne více než 1 kalendářní měsíc ode dne podání Žádosti, je povinna pověřená osoba informovat subjekt údajů a důvodech prodlení s vyřízením Žádosti a dále je povinna subjektu údajů sdělit termín, v němž bude Žádost vyřízena. Žádost musí být bezpodmínečně vyřízena nejpozději do 2 kalendářních měsíců ode dne jejího uplatnění.
4. Na písemnou Žádost odpoví pověřená osoba subjektu údajů písemně doporučeným dopisem. Jestliže subjekt údajů podal Žádost v elektronické formě, poskytne pověřená osoba odpověď na Žádost subjektu údajů e-mailem či elektronicky do datové schránky subjektu údajů, pokud subjekt údajů nepožádá o jiný způsob. Vždy je třeba ověřit identitu toho, kdo žádost v elektronické formě podal, aby se odpověď na Žádost a osobní údaje subjektu údajů nedostaly neoprávněným osobám. V případě pochybností o elektronické nebo faktické adrese je pověřená osoba povinna adresu ověřit u subjektu údajů např. telefonátem, zasláním SMS nebo vyžádáním osobní identifikace subjektu údajů.

5. Vyřízení Žádosti včetně uspokojení odůvodněných práv a nároků (je-li Žádost vyřízena kladně nebo částečně kladně) je bezplatné.

XI. Hlášení porušení zabezpečení osobních údajů

1. Porušením zabezpečení osobních údajů ve smyslu ust. čl. 4 odst. 12 GDPR je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (dále jen „**porušení zabezpečení údajů**“). Porušením zabezpečení údajů jsou např. ztráta mobilního telefonu, ztráta notebooku, ztráta diáře s kontakty zákazníků a dodavatelů, neplánované smazání osobních údajů, ztráta osobních spisů zaměstnanců či spisů vedených pro konkrétní odběratele, dodavatele nebo smluvní partnery, napadení počítače virem, zjištění přístupu k osobním údajům k tomu neoprávněnou osobou, vyhoření serveru s uloženými osobními údaji, zaslání dokumentu obsahujícího osobní údaje neoprávněné osobě apod. Jakékoliv porušení zabezpečení údajů je zaměstnanec povinen obratem (nejpozději do 2 hodin od zjištění porušení zabezpečení údajů) nahlásit svému nadřízenému a pověřené osobě a to včetně popisu takového porušení, jeho rozsahu (druh a množství dotčených osobních údajů) a uvedení dotčených subjektů údajů.

2. V souladu s ust. čl. 33 odst. 1 GDPR je společnost povinna jakékoli porušení zabezpečení údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm společnost dozvěděla, ohlásit 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. Za splnění povinnosti dle předcházející věty tohoto odstavce je odpovědná pověřená osoba. Pověřená osoba je povinna vyhodnotit, zda je porušení zabezpečení údajů nutné hlásit dozorovému úřadu a v případě, že nahlášení je nutné, je povinen tak učinit ve lhůtě 72 hodin, jak je uvedena v první větě tohoto odstavce.

3. V případě nutnosti nahlášení porušení zabezpečení údajů dle odst. 2 tohoto článku směrnice je nutné dozorovému úřadu nahlásit následující informace:
    a. popis povahy daného případu porušení zabezpečení údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
    b. jméno a kontaktní údaje pověřené osoby, která může poskytnout bližší informace;
    c. popis pravděpodobných důsledků porušení zabezpečení údajů;
    d. popis opatření, která společnost přijala nebo navrhla k přijetí s cílem vyřešit dané porušení zabezpečení údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů

Pakliže není možné v rámci lhůty 72 hodin shromáždit veškeré výše uvedené informace, které by měly být nahlášeny dozorovému úřadu, je třeba v této lhůtě nahlásit dozorovému úřadu alespoň do té doby zjištěné informace týkající se porušení zabezpečení údajů a následně kompletní informace dozorovému úřadu doplnit obratem po jejich zjištění.

4. Při hodnocení závažnosti porušení zabezpečení údajů pověřená osoba musí zejména zohlednit, o jaké osobní údaje se jedná (např. citlivé údaje nebo údaje zjistitelné z veřejně dostupných zdrojů), zda byly osobní údaje zabezpečeny (např. zaheslování počítače nebo telefonu při jeho ztrátě, zaheslování a šifrování samotných dat v počítači nebo nosiči dat), o

koho se v případě zpřístupnění osobních údajů k tomu neoprávněné osobě jednalo (např. zaměstnanec bez přístupových údajů nebo pracovník konkurence). Pro hodnocení závažnosti má také vliv snadnost identifikace jednotlivců podle uniknuvších dat, závažnost důsledků pro jednotlivce nebo počet dotčených jednotlivců.

5. Společnost vede evidenci porušení zabezpečených údajů a pověřená osoba do této evidence zaznamenává každé porušení zabezpečení údajů a to bez ohledu na to, zda je porušení zabezpečení údajů hlášeno dozorovému úřadu, případně i subjektu údajů, či nikoliv.
6. Odstranění nežádoucího stavu a nápravu porušení zabezpečení údajů jsou povinni ve vzájemné součinnosti zajistit pověřená osoba společně s osobou, která porušení zabezpečení údajů zjistila, a nadřízeným této osoby.
7. Pokud je pravděpodobné, že určitý případ porušení zabezpečení údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí společnost jako správce toto porušení bez zbytečného odkladu subjektu údajů. Za splnění této povinnosti stejně jako za prošetření a vyhodnocení nutnosti hlásit porušení zabezpečení údajů subjektu údajů odpovídá pověřená osoba. Pro vyhodnocení případné povinnosti hlásit porušení zabezpečení údajů subjektu údajů se postupuje shodně, jak je uvedeno výše v tomto článku směrnice, zejména v odst. 4., s tím, že se povinnost nahlásit porušení zabezpečení údajů subjektu údajů vztahuje pouze na vysoké riziko hrozící v takové souvislosti subjektu údajů. V případě nutnosti ohlášení případu porušení zabezpečení údajů subjektu údajů informuje společnost subjekt údajů v rozsahu shodně s tím, jak je uvedeno v odst. 3 tohoto článku, a dále je pověřená osoba povinna konzultovat s dozorovým úřadem postup informování subjektů údajů.

Vysoké riziko hrozící subjektu údajů v souvislosti s porušením zabezpečení údajů existuje např. v případě, že porušení může u dotčeného jednotlivce vést k tělesné, materiální nebo nemateriální škodě. Příklady takové škody jsou diskriminace, krádež totožnosti nebo podvod, peněžní ztráta a poškození pověsti. Vysoké riziko taktéž souvisí s únikem citlivých údajů (zvláštní kategorie osobních údajů ve smyslu ust. čl. 9 GDPR) jako např. zdravotní stav nebo členství v odborech.

XII. Závěrečná ustanovení

1. Na provádění a dodržování všech povinností a pravidel zpracování osobních údajů a celé této směrnice jsou povinni dohlížet nadřízení zaměstnanci ve vztahu ke svým bezprostředně podřízeným a dále pověřená osoba.
2. Směrnice nabývá platnosti a účinnosti dne 25. 5. 2018.
3. Přílohou a nedílnou součástí této směrnice jsou:

Příloha č. 1 „Informace o zpracování osobních údajů zaměstnanců, uchazečů o zaměstnání a členů orgánu správce“

Příloha č. 2 „Informace o zpracování osobních údajů zákazníků, odběratelů, dodavatelů a smluvních partnerů“

Příloha č. 3 „Informace o zpracování osobních údajů společníků“

Příloha č. 4 „Zkrácená informace o zpracování osobních údajů“

Příloha č. 5 „Souhlas subjektu údajů se zpracováním osobních údajů“

Příloha č. 6 „Žádost – uplatnění práv subjektu údajů“

Příloha č. 7 „Vzor odpovědi na žádost – uplatnění práv subjektu údajů“

V Plzni dne 25. 5. 2018

za **EUFRAT Group, s.r.o.**

Bc. Danuše Burešová, jednatelka