město Mimoň
Mírová 120, Mimoň, Mimoň III, PSČ 471 24, tel. 487805001, fax 487805044,
podatelna@mestomimon.cz

VNITŘNÍ PŘEDPIS O ZPRACOVÁNÍ A OCHRANĚ OSOBNÍCH ÚDAJŮ

podle **§ 305 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů (dále jen „zákoník práce“)** tento

VNITŘNÍ PŘEDPIS

kterým se blíže upravují práva a povinnosti zaměstnanců upravené v 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, v platném znění (dále jen „Nařízení“)**, jakož i vnitřní organizace zaměstnavatele při zpracování osobních údajů**

POČET STRAN: 9

PLATNOST OD: pro rok 2018

	ZPRACOVAL	SCHVÁLIL
Jméno	**Mgr. Bronislava Tvrzníková**	**František Kaiser**
Datum	**21. 5. 2018**	**23. 5. 2018**

I. PŮSOBNOST

Tento vnitřní předpis stanovuje práva a povinnosti zaměstnanců při zpracování osobních údajů, a to jak při ručním, tak automatizovaném zpracování. Vztahuje se na všechny zaměstnance organizace a upravuje komplexně oblast ochrany osobních údajů.

II. DEFINICE A POJMY

Pro účely tohoto vnitřního předpisu se rozumí:

a) Nařízením 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 (obecné nařízení o ochraně osobních údajů).

b) Osobním údajem (dále také jako „OÚ“) každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat.

c) Citlivými osobními údaji (tzv. zvláštní kategorie osobních údajů) údaje, které mohou subjekt údajů samy o sobě poškodit (např. ve společnosti, zaměstnání, škole) či mohou zapříčinit jeho diskriminaci.
Jde zejména o: *národnostní, rasový nebo etnický původ, politické postoje, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofické přesvědčení, údaje o trestné činnosti, zdravotní stav a sexuální život*.

d) Subjektem údajů fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

e) Správcem osobních údajů (dále také „Správce“) Zaměstnavatel. Správci osobních údajů sami nebo společně určují účely (na základě čeho) a prostředky zpracování (formu)

f) Zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který na základě zákona nebo pověření Správce zpracovává osobní údaje pro správce

g) Příjemcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují (inspekční a vyšetřovací orgány jako PČR, FÚ, ČOI, ÚOHS aj.). Zpracování osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

h) Zpracováním osobních údajů 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. Zpracování osobních údajů je nutné považovat za sofistikovanější činnost, kterou správce osobních údajů nebo zpracovatel s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky.

i) Profilováním jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

j) Pseudonymizací zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

k) Anonymizací Zpracování osobních údajů způsobem, že nemohou být již nikdy přiřazeny konkrétnímu subjektu a jeho identifikaci ani nenapomáhají.

l) Souhlasem subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Může být učiněn písemně, elektronicky i ústně.

m) Pověřencem pro ochranu osobních údajů (dále také „DPO“ nebo „pověřenec“) pozice v rámci organizace, v níž působí zaměstnanec nebo externí pracovník jako ochránce osobních údajů zaměstnanců, občanů, klientů, zákazníků, dodavatelů a dalších fyzických osob, jejichž údaje Správce osobních údajů zpracovává. Funguje mj. jako prostředník pro komunikaci mezi subjektem údajů, správcem a dozorovým úřadem.

n) Odpovědnou osobou osoba uvedená v čl. IV. tohoto vnitřního předpisu.

o) Bezpečnostním incidentem porušení zabezpečení / únik dat – náhodné nebo protiprávní zničení, ztráta, změna nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních dat.

p) Kategoriemi OÚ: adresní, identifikační, zvláštní a popisné.

Adresní (kontaktní) a identifikační údaje jsou údaje k jednoznačné a nezaměnitelné identifikaci a umožňující kontakt se subjektem údajů (např. jméno, příjmení, titul, rodné číslo, datum narození, adresa trvalého pobytu, kontaktní nebo doručovací adresa, místo narození, státní příslušnost, pohlaví, u fyzické osoby podnikající též daňové identifikační číslo a IČ, dále kontaktní adresa, číslo telefonu, e-mailová adresa, jméno datové schránky).

Popisné údaje jsou údaje vytvářející komplexní obraz fyzické osoby (například údaje o vzdělání, znalosti cizích jazyků, odborné znalosti a dovednostech, počtu dětí, informace o absolvování vojenské služby, o předchozím zaměstnání, zdravotní pojišťovně, mzdě, ale také vzhled, výška, postava, barva vlasů apod.)

Zvláštní – viz. odstavec II., písm. c)

q) Úřadem je Úřad pro ochranu osobních údajů České republiky (dále také ÚOOÚ).

r) Zaměstnancem se pro účely tohoto vnitřního předpisu rozumí i statutární orgán, pokud je dle čl. IV. odpovědný za plnění povinností dle tohoto vnitřního předpisu.

III. KATEGORIE OSOBNÍCH ÚDAJŮ, ÚČELY A PRÁVNÍ TITULY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. Zaměstnavatel zpracovává tyto kategorie OÚ:
   a) Adresní, identifikační a popisné
   b) Zvláštní, zejména údaje o zdravotním stavu a členství v odborové organizaci, je-li zřízena

2. Zaměstnavatel zpracovává OÚ za účelem plnění pracovněprávních povinností, za účelem plnění smluvních povinností se svými obchodními partnery a pro účely plnění povinností uložených mu platnými zákony.

3. Právním titulem pro zpracování osobních údajů u zaměstnavatele je především plnění zákonných povinností, plnění smlouvy, oprávněný zájem, veřejný zájem a v odůvodněných případech souhlas se zpracováním osobních údajů nebo ochrana životně důležitých zájmů subjektu údajů.

IV. ODPOVĚDNÉ OSOBY

1. Osobou odpovědnou za dodržování povinností Nařízení je u zaměstnavatele starosta města, dále pak vedoucí jednotlivých odborů.

2. Osobou pověřenou implementací a kontrolou bezpečnostních a technicko-organizačních opatření v souvislosti se zpracováním a ochranou OÚ je: Tajemnice úřadu.

3. Pro účely kontaktování pověřené osoby v případech dotazů, námitek a žádostí souvisejících s bezpečností, ochranou a zpracováním osobních údajů a hlášení bezpečnostních událostí a incidentů se stanovují tyto kontaktní údaje:
   e-mailová adresa: kabes@mestomimon.cz

   Za vyřízení zákonných žádostí a námitek došlých na uvedený e-mail je odpovědný Bc. Matyáš Kabeš

4. V ostatních případech je za dodržení povinností uvedených v této směrnici odpovědný zaměstnanec, který OÚ zpracovává a kterého zaměstnavatel pověřil úkoly spojenými s ochranou OÚ v rámci jeho organizační struktury.

5. Pověřencem pro ochranu osobních údajů je jmenován: Bc. Matyáš Kabeš
   Kontaktní e-mail: kabes@mestomimon.cz

Kontaktní telefonní číslo: 724 066 017

V. PRÁVA A POVINNOSTI

Povinnosti zaměstnanců

1. Všichni zaměstnanci jsou povinni při výkonu práce zajistit, aby nebyly OÚ zpřístupněny neoprávněným příjemcům a dodržovat mlčenlivost o OÚ všech subjektů údajů, se kterými přijde při výkonu práce do styku. Zaměstnanec zpracovává OÚ subjektů údajů pouze na pokyn zaměstnavatele zákonně, korektně, transparentně, k účelu, ke kterému byly údaje subjektem údajů poskytnuty, v minimálním nezbytném rozsahu, přesně, po dobu ne delší, než je nezbytné pro účel zpracování, a způsobem, který zajistí náležité zabezpečení OÚ včetně jejich ochrany.

2. Zaměstnanec musí dodržovat mlčenlivost o svých přístupových údajích a heslech do počítačových systémů zaměstnavatele. Zaměstnanec je povinen listinné nosiče OÚ (dokumenty) v době, kdy s nimi nepracuje, odpovídajícím způsobem zabezpečit před neoprávněným přístupem, poškozením, zneužitím či ztrátou. Zaměstnanec je povinen se odhlásit (uzamknout) z počítačového systému při vzdálení se od počítače zaměstnavatele, na kterém pracuje a zabezpečit svěřenou techniku před neoprávněným přístupem.

3. Jsou-li zpracovávány OÚ na základě souhlasu subjektu údajů, musí být souhlas písemný a musí být uložen v listinné nebo elektronické podobě, aby byl doložitelný. Zaměstnanec, který souhlas připravuje, je povinen jako výchozí vzor použit souhlas, který je Přílohou 3 a vždy informovat subjekt údajů, že souhlas je odvolatelný zasláním žádosti na oficiální e-mailovou adresu podatelny, poštovní adresu zaměstnavatele.

4. Zpracovává-li zaměstnanec OÚ subjektu údajů mladšího 18 let v případech, kdy není zpracování stanoveno právní povinností, je povinen tak činit se souhlasem a schválením zákonného zástupce – rodiče subjektu údajů. Zaměstnanec vyvine přiměřené úsilí, aby ověřil, že souhlas byl dán opravdu rodičem.

5. Zakazuje se zpracování OÚ, které vypovídají 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, nejde-li o zákonem stanovené výjimky spočívající ve vedení personálních agend nebo plnění úkolů nezbytných pro splnění úkolů daných platnými zákony.

Práva subjektu údajů

1. Získává-li zaměstnanec OÚ od subjektu údajů, splní vůči subjektu údajů informační povinnost o jeho právech a poskytne potřebná sdělení, kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

2. Zaměstnanec, který je zaměstnavatelem pověřen komunikací se subjekty údajů v případech, kdy realizují svoje práva, poskytne subjektu údajů na žádost o přístup, žádost o informaci, zda a jaké OÚ se zpracovávají, opravu, výmaz, omezení zpracování, přenositelnost OÚ nebo vznese-li námitku či požádá-li o zrušení automatizovaného zpracovávání či profilování informace o přijatých opatřeních do jednoho měsíce od obdržení žádosti, jinak informuje subjekt údajů bezodkladně, nejpozději do 1 měsíce, o důvodech nepřijetí opatření a o možnosti podat stížnost u Úřadu pro ochranu osobních údajů.

3. Nezískává-li zaměstnanec OÚ od subjektu údajů, splní vůči subjektu údajů informační povinnost, kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

4. Zaměstnanec vymaže OÚ, jestliže:
   a) OÚ již nejsou potřebné,
   b) jestliže subjekt údajů odvolá souhlas a neexistuje žádný další důvod pro zpracování,
   c) subjekt údajů vznese námitky proti zpracovávání OÚ na základě oprávněného zájmu Správce nebo proti automatizovanému individuálnímu rozhodování nebo proti profilování,
   d) jestliže OÚ byly zpracovávány protiprávně,
   e) jestliže OÚ musí být vymazány ke splnění právní povinnosti,

   kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

Jestliže má být OÚ vymazán, zaměstnanec informuje zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby je vymazali.

5. Zaměstnanec je povinen předem upozornit subjekt údajů, kterému bylo omezeno zpracování OÚ, že omezení bude zrušeno.

6. Zaměstnanec je povinen oznámit veškerým příjemcům, jimž byly OÚ zpřístupněny, veškeré opravy, výmazy, omezení s výjimkou toho, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Zaměstnanec informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje, kromě případů, kdy mu právní předpis nebo pokyn zaměstnavatele ukládá jiný postup.

7. Zaměstnanec vyřizuje námitky subjektu údajů proti zpracování OÚ, které se ho týkají, a byly získány ke splnění úkolu ve veřejném zájmu nebo na základě oprávněného zájmu Zaměstnavatele, včetně profilování, námitky proti zpracování OÚ pro přímý marketing, které se ho týkají, což zahrnuje i profilování.

VI. TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

1. Zaměstnavatel provádí následující opatření:

a) Vstupní analýza zpracování OÚ – Před účinností tohoto vnitřního předpisu a ke správnému nastavení opatření provedl zaměstnavatel analýzu současného stavu zpracovávání osobních údajů.

b) Kybernetická bezpečnost – Zaměstnavatel zpracovává OÚ v elektronické podobě pomocí informačních systémů a webových aplikací, které fungují v prostředí Linux a Microsoft Windows. Uživatelem jsou jen zaměstnanci, kteří se do prostředí a informačních systémů přihlašují uživatelským jménem a heslem. OÚ představující vysoké riziko zaměstnavatel šifruje, pseudonymizuje nebo chrání dalšími technickými opatřeními odpovídajícími míře rizika zpracovávaných údajů. Pro zpracování OÚ jsou využívány tyto aplikace: GINIS, FLUX, KEOX, SSB a další aplikace v rámci využívání operačního systému Microsoft Windows a kancelářského balíku Microsoft Office.

c) OÚ v elektronické podobě jsou ukládány na zabezpečených úložištích. Zabezpečení je realizováno formou aktualizovaného antivirového programu, dalšími bezpečnostními patřeními případně bezpečnostními politikami, jakož i firewallem a dalšími obrannými systémy serveru a ochranou počítačové sítě proti útokům z internetu. Současně je prováděno zálohování dat na sítový disk NAS Synology DS1515.

d) Elektronická komunikace probíhá prostřednictvím zabezpečeného e-mailového serveru, datové schránky a v nutných případech se zaručeným elektronickým podpisem, kterým zaměstnavatel a vybraní zaměstnanci disponují.

e) Analýza rizik – Zaměstnavatel provedl analýzu relevantních rizik v oblasti ochrany a zpracování OÚ.

f) Fyzická bezpečnost – Zaměstnavatel zpracovává OÚ v listinné podobě na nosičích OÚ. Zaměstnanci dodržují ochranu OÚ tak, že minimalizují množství OÚ, které zpracovávají, listinné nosiče OÚ zamykají do stolních zásuvek, spisoven, skříní apod. a kanceláře a vstup do prostor využívaných pro ukládání a zpracovávání osobních údajů chrání elektronickým zabezpečovacím systémem.

g) Omezení přístupu k OÚ prostřednictvím vymezení kompetencí v rámci organizační struktury zaměstnavatele, kdy přístup k datům obecně je diferencován dle oddělení

a pracovního zařazení. Statutární orgány mají přístup k veškerým datům a informacím.

h) Omezení přístupu k některým adresářům a aplikacím (programům) jen pro vymezený okruh oprávněných osob.

i) Vzdělávání zaměstnanců. Zaměstnavatel zvyšuje povědomí odpovědných zaměstnanců školením o jejich povinnostech v souvislosti s ochranou subjektů údajů při zpracování jejich OÚ, zejména pak seznámením s obsahem tohoto vnitřního předpisu.

j) Periferní mobilní zařízení jako jsou chytré telefony a tablety připojené na informační systémy, servery nebo do sítě zaměstnavatele např. za účelem vyřizování elektronické pošty jsou používány tak, že na každém z nich je nainstalován nejméně antivirový systém a zaměstnanci dodržují bezpečnostní politiky a obecné zásady bezpečnosti spojené s přístupem do informačních systémů zaměstnavatele prostřednictvím těchto mobilních zařízení.

2. Zaměstnanec je oprávněn předat OÚ jen zpracovateli, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření.

3. Zaměstnanec, který má poskytnout OÚ ke zpracování zpracovateli, je povinen prověřit, zda má zaměstnavatel se zpracovatelem uzavřenou písemnou smlouvu o zpracování osobních údajů a případně uzavření takové smlouvy, jejíž vzor je v Příloze 1, iniciovat.

4. Zaměstnavatel provádí jednou ročně testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování OÚ.

5. Součástí pracovního nebo organizačního řádu a pracovní náplně zaměstnanců majících přístup k OÚ je doložka o mlčenlivosti a ochraně OÚ a součástí smluv se zpracovateli doložka obdobného obsahu. Popřípadě je v tomto smyslu uzavírána zvláštní dohoda o ochraně OÚ a mlčenlivosti.

6. Jakékoli porušení zabezpečení OÚ každý zaměstnanec neprodleně, nejpozději však do 24 hodin od okamžiku, kdy se o porušení dozvěděl, oznámí svému nadřízenému nebo pověřené osobě, případně odpovědným osobám/statutárnímu zástupci uvedeným v odstavci IV. ODPOVĚDNÉ OSOBY tohoto předpisu.

7. Statutární zástupce nebo pověřená osoba nejpozději do uplynutí 72 hodin od okamžiku, kdy byl bezpečnostní incident poprvé v organizaci zaznamenán, oznámí takové porušení zabezpečení/únik dat Úřadu. Proces oznámení konzultuje s DPO nebo pověří DPO řízením procesu oznámení incidentu Úřadu. Statutární orgán

dokumentuje veškeré případy porušení, účinky a přijatá nápravná opatření. Dojde-li k porušení zabezpečení OÚ zpracovávaných elektronicky, odpovědný zaměstnanec do 24 hodin informuje osobu, která spravuje informační systémy, aby zjistila narušitele a do 48 hodin navrhla nápravné opatření. Při řešení bezpečnostních incidentů zaměstnavatel spolupracuje se správcem sítě, osobou pověřenou implementací a kontrolou bezpečnostních a technicko-organizačních opatření v souvislosti se zpracování a ochranou OÚ.

8. Pokud je pravděpodobné, že určitý případ porušení zabezpečení OÚ bude mít za následek vysoké riziko pro práva a svobody subjektu údajů, oznámí to pověřený zaměstnanec bez zbytečného odkladu subjektům údajů.

VII. ZVLÁŠTNÍ USTANOVENÍ

a) Zaměstnavatel je povinen jmenovat pověřence pro ochranu osobních údajů, neboť po provedené analýze provádí rozsáhlé pravidelné a systematické monitorování OÚ a současně je v pozici orgánu veřejné moci nebo orgánu zřízeného zákonem, který plní zákonem stanovené úkoly ve veřejném zájmu.

b) Zaměstnavatel dále není povinen provádět posouzení vlivu na ochranu OÚ, neboť není pravděpodobné, že druhy zpracování OÚ jím prováděné představují vysoké riziko pro práva a svobody subjektů údajů, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování OÚ.

c) Zaměstnavatel není povinen provádět záznamy o činnostech zpracování OÚ, neboť počet jeho zaměstnanců není vyšší než 250 a při zpracování OÚ nevzniká vysoké riziko pro práva a svobody subjektů údajů.

VIII. LHŮTY PRO VÝMAZ

1. Lhůty pro výmaz OÚ se řídí právní řádem České republiky a případně spisovým řádem zaměstnavatele.

IX. ÚČINNOST

Tento vnitřní předpis nabývá účinnosti dne 25. 05. 2018, přičemž byl zveřejněn způsobem, který je v souladu s příslušnými ustanoveními zákoníku práce, vč. seznámení zaměstnanců s jeho obsahem.

Přílohy:
Příloha č. 1 – Zpracovatelská smlouva
Příloha č. 2 – Souhlas se zpracováním

V Mimoni dne 23. 5. 2018