

Příručka ochrany osobních údajů pro zaměstnance Stavebního bytového družstva Studénka – Butovice

1	Úvod	1
2	Bezpečnost informací	2
3	Povinnosti osob pověřených zpracováním osobních údajů	3
4	Pravidla pro zaměstnance při automatizovaném zpracování osobních údajů	4
5	Sankce	5

Článek 1 - Úvod

1. Základní pojmy

Správce osobních údajů: Stavební bytové družstvo Studénka – Butovice, se sídlem Školní 53, 742 13 Studénka (dále jen SBD).

Zpracování je jakákoli operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Subjektem údajů je fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba.

Správce je subjekt, nerozhoduje, jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá.

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce.

Zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby.

2. Zásady a právní důvody zpracování

Zásady ochrany osobních údajů dle GDPR lze ve stručnosti shrnout na:

- zákonnost, korektnost, transparentnost – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně

a korektně,

- omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
- minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
- přesnost – osobní údaje musí být přesné,
- omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
- integrita a důvěrnost – technické a organizační zabezpečení osobních údajů.

Právní důvody zpracování osobních údajů znamenají oprávnění správce osobní údaje zpracovávat.

Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních důvodů:

- subjekt údajů udělil souhlas pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

3. Práva subjektu údajů

Subjekt údajů má právo na to být informován o zpracování svých osobních údajů a další práva, která jsou mnohdy založena na žádosti subjektu údajů, zejména:

- právo na přístup k osobním údajům,
- právo na opravu, resp. doplnění,
- právo na výmaz,
- právo na omezení zpracování,
- právo na přenositelnost údajů,
- právo vznést námitku,
- právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnující i profilování.

Článek 2 – Bezpečnost informací

Zabezpečení osobních údajů

Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s platnými právními předpisy pro oblast ochrany osobních údajů. Každý správce tak bude muset přijmout adekvátní bezpečnostní opatření a u každého správce takové opatření může být, právě

s ohledem na povahu, rozsah a účely zpracování, odlišné.

1. Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být zabezpečeny pod uzávěrou, popř. na jiných místech, kde je možno zajistit jejich ochranu. To platí i pro kopie písemností obsahující osobní údaje.
2. Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů.
3. Za plnění povinností stanovených v tomto metodickém postupu jsou odpovědní zaměstnanci podle rozsahu svých oprávnění.
4. Za likvidaci písemností a záznamových médií odpovídají zaměstnanci. Za likvidaci dat v rámci informačních systémů pro zpracování osobních údajů zodpovídá správce IT.

Článek 3 – Povinnosti osob pověřených zpracováním osobních údajů

Zaměstnanci jsou povinni v rámci plnění svých povinností vyplývajících z jejich vztahu k SBD plnit také opatření k ochraně osobních údajů stanovené právními předpisy, tímto a dalšími vnitřními předpisy SBD, zejména:

1. Zachovávat mlčenlivost o osobních údajích a přijatých technicko - organizačních opatřeních k jejich ochraně, o nichž se v souvislosti se svým zaměstnáním dozvěděli, a to i po skončení svého pracovního poměru.
2. Zpracovávat osobní údaje za podmínek a v rozsahu jim stanoveném (např. v souladu s platnými přístupy do systémů pro automatizované zpracování OÚ), a to v rozsahu:
 - a) stanoveném zvláštním právním předpisem,
 - b) není-li rozsah zvláštním právním předpisem stanoven, pak v rozsahu nezbytně nutném k naplnění stanového účelu.
3. Při shromažďování osobních údajů od subjektů údajů:
 - a) vyžadovat jejich souhlas se zpracováním osobních údajů (není-li zpracování osobních údajů dáno zvláštním zákonem),
 - b) informovat a poučit je o jejich právech v souladu se zákonem,
 - c) shromažďovat osobní údaje pouze otevřeně, tj. neshromažďovat osobní údaje skrytě nebo pod záminkou jiného účelu.
4. Při zpracování osobních údajů:
 - a) zpracovávat pouze přesné osobní údaje s ohledem na účel zpracování; v případě zjištění, že zpracovávané osobní údaje nejsou přesné, zpracování zablokovat do doby jejich opravy nebo doplnění,
 - b) zpracovávat osobní údaje pouze k účelům, k nimž byly shromážděny (k jinému účelu pouze v případě, že fyzická osoba, ke které se osobní údaje vztahují, dala k tomu předem souhlas),
 - c) nesdružovat osobní údaje získané k rozdílným účelům,
 - d) uchovávat osobní údaje pouze po dobu, která je nezbytně nutná k účelu zpracování,
 - e) ukládat nosiče obsahující osobní údaje, a to v listinné i elektronické podobě, na určená místa. Při práci s nosiči postupovat tak, aby jiná osoba nemohla zneužít tyto nosiče jako zdroj informace (dle zásad „čistého stolu“ a „prázdné obrazovky“).
5. Nepořizovat kopie nosičů s osobními údaji či osobních údajů samých pro jinou než pracovní potřebu a ani to umožňovat jiným; s takovými kopiemi nakládat stejně jako s originálem.

6. Neumožnit zpracování osobních údajů jiné osobě, která není pro konkrétní účel zpracování pověřenou osobou.
7. Osobní údaje v listinné i elektronické formě, předávat nebo poskytovat:
 - a) pouze pověřeným a oprávněným osobám,
 - b) stanoví-li tak zvláštní zákon nebo v souladu s platnou smlouvou,
 - c) pouze předepsaným způsobem.
8. V případě zjištění porušení bezpečnostních opatření k zajištění ochrany osobních údajů informovat bez zbytečného odkladu vedoucího zaměstnance a garanta ochrany osobních údajů.

Článek 4 - Pravidla pro zaměstnance při automatizovaném zpracování osobních údajů

1. Zákaz

Informace SBD lze používat jen k plnění povinností vyplývajících z pracovní smlouvy s SBD. Neveřejné informace, včetně předmětu obchodního tajemství, osobních údajů musí každý zaměstnanec uchovávat v tajnosti a učinit veškerá možná opatření, zabraňující jejich zneužití či prozrazení.

Všechny komponenty počítačové sítě jsou vlastnictvím SBD, případně k nim SBD vlastní či vykonává práva užívání. Zákaz krádeže a vandalizmu (poškození) se pak vztahuje na elektronickou podobu dat a informací stejně jako na vlastní fyzické prostředky.

Především je zakázáno:

- a) Používat k provozu v síti SBD nepovolené zařízení, nebo zařízení nedostatečně zabezpečené (bez aktualizací operačního systému nebo antivirového programu apod.).
- b) Svěvolně instalovat a používat neevidované programové vybavení, nebo instalační soubory neevidovaných programů ukládat na pevném disku.
- c) Šířit, nebo se snažit získat nelegální software.
- d) Pracovat s uživatelským jménem a heslem, které mu nebylo přiděleno.
- e) Obcházet bezpečnostní funkce. Bránit operačnímu systému nebo antivirovému programu v provádění automatických aktualizací.
- f) Neautorizované a neschválené kopírování i částí programového vybavení nebo dat, k nimž SBD vykonává vlastnická práva, resp. práva k užívání.
- g) Neautorizovaná modifikace programů, dat nebo technického vybavení v majetku či užívání SBD. Zvláště přísně jsou pak zakázány neautorizované změny konfigurace počítačů či jiných prostředků, které by mohly mít vliv na provoz celé sítě.
- h) Poškození nebo zničení počítačových prostředků (počítačů, programového vybavení i komunikačních linek).
- i) Odposlouchávání provozu a vytváření kopií zpráv či dat procházejících jednotlivými uzly sítě.
- j) Instalovat programy nebo technická zařízení, která monitorují činnost jiných uživatelů nebo serverů, případně jinak zasahovat do oblasti sítě.
- k) Využívat síť SBD ke komerčním účelům, nebo rozesílat nevyžádanou poštu (SPAM).
- l) Použití počítačových prostředků SBD k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě nebo sítě Internet.

2. Zodpovědnost

Uživatel zodpovídá za:

- a) Zachování mlčenlivosti a uchování v tajnosti všech neveřejných informací SBD.
- b) Úplnost přiděleného zařízení a jeho správné používání.
- c) Dodržování bezpečnostních zásad práce v síti SBD a na přiděleném zařízení.
- d) Dodržování zásad SBD při zpracování, ukládání a manipulaci s daty.
- e) Používání legálního a řádně evidovaného software.
- f) Škody způsobené úmyslně či z nedbalosti.

Uživatel je povinen

- a) Pro přístup do sítě SBD používat pouze povolené zařízení a přidělené přihlašovací údaje.
- b) Dodržovat zejména tato pravidla provozu v síti:
 - a. Používat pouze legální a řádně evidované programové vybavení instalované oprávněným pracovníkem,
 - b. Při virové nákaze nebo neobvyklém chování zařízení jej okamžitě odpojit od sítě, a tuto skutečnost neprodleně nahlásit vedoucímu pracovníkovi,
 - c. Při zjištění porušení zásad stanovených touto směrnicí a směrnicí pro uživatele, nebo při podezření na zneužívání sítě SBD okamžitě informovat správce IT a vedoucího pracovníka.

3. Postupy

Oprávnění k užívání informačního systému.

- a) Pracovník se stává uživatelem získáním oprávnění k užívání informačního systému. Uživatel, kterému je účet zřízen, získá heslo a je povinen toto heslo udržovat v tajnosti.
- b) V případě prozrazení hesla (či sebemenší domněnce, že jeho heslo bylo prozrazeno) neprodleně informuje správce IT a vedoucího pracovníka a zažádá o změnu hesla.

Pro používání hesel platí zejména tato pravidla:

- a) Heslo musí být uchováno v tajnosti a zodpovědnost za všechny činnosti, související s použitím identifikátoru a hesla, má jeho vlastník.
- b) Heslo k vlastnímu účtu uživatel nesmí sdělit druhé osobě.
- c) Heslo musí být zvoleno tak, aby nebylo snadné je odhalit.
- d) Nepoužívají se běžná slova, jména nebo čísla spojená s uživatelem, a to ani jejich kombinace.
- e) Heslo by mělo být pravidelně měněno, nejméně tehdy, když existuje možnost, že mohlo být vyzrazeno.
- f) Nedoporučuje se používat stejný login a heslo v aplikaci SBD a v aplikaci na internetu.
- g) Nedoporučuje se používat stejné heslo do několika aplikací.
- h) Nedoporučuje se zapisovat svoje heslo na papír. Pokud je heslo zapsáno, musí být bezpečně uschováno např. v zalepené obálce v trezoru.
- i) Nedoporučuje se použití funkcí a programů pro zapamatování hesel, použití kombinace kláves pro vyvolání hesla apod.
- j) V případě, kdy jsou dodávány technické nebo programové prostředky s heslem nastaveným výrobcem, musí být toto heslo okamžitě po převzetí (instalaci) změněno.
- k) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností uživatele změnit toto heslo při prvním přihlášení.

Článek 5 – Sankce

Porušení ustanovení této směrnice může být u zaměstnanců považováno až za závažné porušení povinností vyplývající z právních předpisů vztahujících se k zaměstnancem

vykonávané práci (§ 52 g), Zákoníku práce) a lze z něj vyvodit příslušné pracovněprávní důsledky včetně okamžitého rozvázání pracovního poměru. V případě vzniklé škody bude částka předepsána osobě zodpovědné za škodu k úhradě.