

Technická a bezpečnostní opatření

Technická a bezpečnostní opatření jsou ve Společnosti tvořena zejména následujícími pravidly a/nebo opatřeními:

- opatřeními pro zabezpečení elektronických systémů;
- opatřeními pro zabezpečení listin;
- vnitřními předpisy Společnosti a pokyny vedoucích zaměstnanců.

Zabezpečení elektronických systémů

Za účelem zajištění bezpečnostních opatření pro nakládání s osobními údaji v elektronické podobě, Společnost zavedla opatření zejména pro následující oblasti elektronických systémů:

a. Centrální IT infrastruktura

Technické zabezpečení pracovišť pro zpracování osobních údajů subjektů správce:

Automatizované zpracování dat se provádí na zařízeních, která jsou proti neoprávněným zásahům zvenčí či jinému zneužití dat chráněna takto: Počítačová síť zpracovatele BIC Plzeň v sídle společnosti - Riegrově 1 umožňuje sdílení dat z cloudového serveru společnosti Microsoft - SharePoint, zde je aplikováno zabezpečení ve standardu společností Microsoft. Správu datové sítě a jejích uživatelů zajišťuje pro BIC Plzeň externě Správa informačních technologií města Plzně. Každý uživatel má přidělené uživatelské jméno a heslo. Bez uživatelského jména a hesla není možné se do vnitřní sítě ani k serveru připojit. Vnitřní počítačová síť je od internetu oddělena firewallem. Centrální prvky sítě jsou instalovány v uzamykatelném rozvaděči. Datový rozvaděč je umístěn v samostatné uzamykatelné místnosti. Prostory BIC jsou zabezpečeny elektronickým zabezpečovacím systémem.

Přístup k datům mají pouze zpracovatelem určené, prověřené a bezúhonné osoby, a to na základě pracovní náplně a nastavených přístupových oprávnění.

Jednotliví zaměstnanci mají jednoznačně vymezené svoje pracoviště.

b. Uživatelské přístupy

Pro správu uživatelských účtů jsou stanovena pravidla upravující způsob založení účtu, rozsah přístupu konkrétního zaměstnance k datům Společnosti či následné zablokování přístupu v případě ukončení pracovního poměru.

c. Koncová zařízení – pracovní počítače na pracovišti

Pro přihlášení do pracovního počítače musí zaměstnanec mít zřízený uživatelský přístup v rozsahu potřebném pro výkon jeho práce. Společnost průběžně dohlíží nad zabezpečením pracovních počítačů, aby nedocházelo mj. k zavírování či jakémukoliv přístupu z jiné sítě.

d. Koncová zařízení – notebooky, tablety, mobilní telefony

Pro notebooky platí pravidla uvedená výše. S ohledem na to, že tato zařízení mohou být užívána i mimo prostory Společnosti, jsou pro jejich zabezpečení nastavena přísnější pravidla, pokud jde zejména o možnost přihlášení se k síti Společnosti či pravidla pro případ ztráty či odcizení. Společnost přijímá a v případě potřeby aktualizuje opatření pro případ ztráty či odcizení notebooku.

Přístup do všech uvedených zařízení je zabezpečen hesly, jejichž správu ve spolupráci s externím poskytovatelem IT služeb řeší pověřený pracovník společnosti.

Zabezpečení fyzických dokumentů

Pro nakládání s osobními údaji v papírové podobě Společnost přijala zejména následující opatření:

- veškeré dokumenty jsou zaměstnanci povinni uchovávat na místech, kam je zamezen přístup nepovolaných osob (v uzamčených skříňkách), přístup k těmto písemnostem je omezen pouze na zaměstnance, kteří s nimi pracují v rámci svých pracovních úkolů,
- vyřízené spisy a jiné dokumenty jsou po dobu trvání skartační lhůty uloženy v samostatné místnosti - v uzamčeném archivu s povoleným přístupem pouze pověřených osob,
- po opuštění pracoviště musí být prostory Společnosti příslušným zaměstnancem zamčeny a elektronicky zakódovány.

Vnitřní předpisy Společnosti

Společnost vydala zejména následující vnitřní předpisy a/nebo pokyny či pracovní postupy, které musí zaměstnanci Společnosti dodržovat, mající dopad i na problematiku zpracování osobních údajů a zajištění jejich ochrany:

- Do styku se zpracovávanými osobními údaji přicházejí jen ti zaměstnanci zpracovatele, kteří byli zpracovatelem poučeni o svých právech a povinnostech, které jim z pracovní činnosti u zpracovatele při zpracování osobních údajů vyplývají, a to zejména v souvislosti s ustanovením zákona č. 110/2019 Sb. a jiných souvisejících právních předpisů.
- Zejména jsou povinni:
 - Přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracovávání osobních údajů.
 - Dodržovat přijatá opatření a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.
 - Zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnaneckého nebo obdobného poměru nebo příslušných prací.

Společnost průběžně reviduje a aktualizuje výše uvedené vnitřní předpisy a/nebo pokyny či pracovní postupy. Se všemi změnami budou zaměstnanci vždy seznámeni.