12. 2. 2021

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Užití chytrých zařízení v pracovněprávních vztazích a ochrana dat

S rozmachem digitálních technologií se i zaměstnanci a zaměstnavatelé potýkají s fenoménem chytrých telefonů a jiných zařízení. Tato zařízení sbírají množství osobních údajů svých uživatelů, tedy zaměstnanců (např. geolokační či biometrické údaje), i data zaměstnavatele či jeho obchodních partnerů (např. pomocí e-mailu), která mohou mít i povahu obchodního tajemství dle § 504 zákona č. 89/2012 Sb., občanský zákoník („OZ“).

Často jsou tato zařízení poskytnuta zaměstnavatelem, např. formou benefitu. Zaměstnanci ale čím dál častěji používají k výkonu práce svá vlastní zařízení. V obou případech mají zaměstnanec i zaměstnavatel určitá práva a povinnosti, která bychom Vám chtěli stručně představit v tomto článku.

Chytrá zařízení poskytovaná zaměstnavatelem

V prvním případě poskytuje zaměstnavatel zaměstnanci nejčastěji telefon či notebook (potažmo tablet) k výkonu závislé práce. Lze se již setkat i s poskytnutím chytrých hodinek, ovšem zatím spíše jako daru zaměstnanci než jako pracovního prostředku. Jelikož zaměstnavatel tato zařízení zaměstnancům pouze „propůjčuje“, má zájem na jejich ochraně a užívání v souladu s jeho pokyny. Je otázkou, jakým způsobem a za jakých okolností může zaměstnavatel kontrolovat zaměstnance při používání těchto zařízení.

Kontrolu zaměstnavateli umožňuje primárně § 316 odst. 1 zákona č. 262/2006 Sb., zákoník práce („**ZP**“), avšak s jistými omezeními. Primárně totiž upravuje zákaz, dle kterého zaměstnanec nesmí bez výslovného souhlasu zaměstnavatele užívat poskytnutá zařízení pro svou osobní potřebu. Zaměstnavatel je v souladu s tímto zákazem oprávněn přiměřeně kontrolovat, zda zaměstnanec tento zákaz dodržuje, nepoužívá zařízení pro osobní potřebu, využívá je k vykonávání svěřených prací, řádně s nimi hospodaří, střeží je a ochraňuje před ztrátou, zničením či zneužitím.

Zaměstnavatel tak může např. přiměřeně sledovat aktivity zaměstnance na internetu, které nesouvisejí s výkonem práce. I když to ZP výslovně nepožaduje, zaměstnavatel by měl zaměstnance o možnosti provádění kontrol předem informovat. Vhodným, efektivním a ve většině případů právně bezvadným řešením může být předchozí blokace určitých pro výkon práce nepoužitelných stránek, domén a sociálních sítí. Pokud zaměstnanec tento zákaz nedodrží, jde o porušení pracovních povinností a zaměstnavatel z toho může vyvodit patřičné důsledky.

Pokud zaměstnavatel udělí zaměstnanci souhlas zařízení užívat i pro osobní potřebu, ztrácí tím možnost kontrolovat na základě § 316 odst. 1 ZP využívání zařízení a aktivity zaměstnance na internetu. Zařízení však stále patří zaměstnavateli a obsahuje data zaměstnavatele či jeho obchodních partnerů. Málokterý zaměstnavatel je proto ochoten rezignovat na jakoukoliv kontrolu nakládání s daným zařízením a daty v něm obsaženými.

Zákon zaměstnavateli jisté možnosti dává. Dle § 316 odst. 2 ZP může zaměstnavatel zaměstnance podrobit otevřenému nebo skrytému sledování, odposlechu a záznamu telefonických hovorů,

kontrole elektronické pošty či listovních zásilek. Musí však splnit striktní podmínky, které toto ustanovení klade. Těmi jsou (i) objektivně závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, (ii) přímé informování zaměstnance o rozsahu kontroly a o způsobech jejího provádění a (iii) provádění kontroly pouze na pracovišti a ve společných prostorách zaměstnavatele. Striktní výklady uvádějí jako příklad, kdy jsou dány závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele, provoz jaderné elektrárny, jiné nebezpečné provozy či věznice. Benevolentnější interpretace uvádějí např. i nakládání se zásadním know-how zaměstnavatele. Záleží ovšem na komplexním posouzení každého jednotlivého případu.

Kontrola musí být přiměřená legitimním zájmům zaměstnavatele, kterých nelze dosáhnout méně invazivním způsobem a které převažují nad zájmy zaměstnance na ochranu soukromí. Je nezbytné dodat, že zaměstnavatel nesmí monitorovat a zpracovávat obsah telefonické, e-mailové a listinné komunikace zaměstnanců, pouze metadata. [1]

Ať již zaměstnavatel provádí kontrolu dodržování zákazu dle § 316 odst. 1 ZP či sleduje zaměstnance dle § 316 odst. 2 ZP, dochází ke zpracovávání osobních údajů a zaměstnavatel má povinnost postupovat v souladu s nařízením (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („**GDPR**“).

Chytrá zařízení ve vlastnictví zaměstnance

V druhém případě zaměstnanec při výkonu závislé práce využívá své vlastní zařízení. Pro tento model se používá označení BYOD (Bring your own device). Nejčastěji jde o počítač nebo mobilní telefon, ale opět je možné si představit i využití chytrých hodinek, které zaměstnanci umožňují vyšší míru propojení. V každém případě se musí jednat o zařízení, které je třeba k výkonu závislé práce.

Právo využití vlastního zařízení při výkonu závislé práce nezakazuje. Stanoví však jisté mantinely. Ty vycházejí především z povahy závislé práce, která musí být vykonávána na náklady zaměstnavatele. Zaměstnavatel tak nemůže zaměstnanci nařídit používání zaměstnancova zařízení. V případě použití zařízení zaměstnance pak bude zaměstnanci náležet náhrada.

Zákonodárce v § 190 ZP předpokládá určení bližších podmínek užívání zařízení zaměstnance v individuální dohodě, vnitřním předpisu či jednostranném písemném určení. Dohoda, vnitřní předpis nebo písemné určení rovněž stanoví podmínky, výši a způsob náhrady. Ta musí vycházet z ceny zařízení, rozsahu jeho používání a musí zohlednit dobu, kdy zaměstnanec zařízení pro pracovní účely nepoužívá. Nutno dodat, že zaměstnanci náhrada nenáleží, pokud použil vlastní zařízení bez souhlasu zaměstnavatele.[2]

V případě BYOD odpadá právo zaměstnavatele kontrolovat využívání zařízení dle § 316 odst. 1 ZP, neboť zákaz dle § 316 odst. 1 ZP zde z logiky věci neplatí. V případě, že jsou pro to splněny podmínky, je možné přiměřenou kontrolu vykonávat postupem dle § 316 odst. 2 ZP, jak je rozebráno výše. I v případě BYOD může zaměstnavatel zpracovávat osobní údaje zaměstnanců. Potom musí zaměstnavatel dodržet povinnosti dle GDPR.

Povinnosti zaměstnavatele dle GDPR

Dle GDPR má zaměstnavatel povinnost zpracovávat osobní údaje zaměstnanců na základě zákonného důvodu, korektně, transparentně, pro výslovně vyjádřené a legitimní účely, v rozsahu nezbytném pro tento účel a pouze po nezbytnou dobu. Zákonným důvodem může být souhlas zaměstnance, plnění pracovní smlouvy, plnění právních povinností zaměstnavatele, ochrana životně důležitých zájmů zaměstnance či jiné fyzické osoby, plnění úkolu ve veřejném zájmu či výkon veřejné moci a ochrana či naplnění oprávněných zájmů zaměstnavatele či třetí strany, pokud mají přednost před zájmy a

základními právy zaměstnance.

V souvislosti s pracovními prostředky mohou být legitimními účely a zároveň oprávněnými zájmy zaměstnavatele zakládajícími zákonnost zpracování osobních údajů zaměstnance právě případy kontroly dle § 316 odst. 1 a odst. 2 rozebírané výše. V takovém případě je zpracování osobních údajů zaměstnance omezeno pouze na tyto účely. Ve většině případů tak bude vyloučeno, aby zaměstnavatel zpracovával např. data o fyzické aktivitě zaměstnance, která zaměstnanec nahrál propojením soukromých chytrých hodinek s pracovním telefonem.

Za určitých okolností může zákonnost zpracování osobních údajů založit i výslovný souhlas zaměstnance. Souhlas musí být dobrovolný a odvolatelný. V pracovněprávních vztazích je však právě otázka dobrovolnosti sporná, neboť zaměstnanec je již z povahy závislé práce podřízen zaměstnavateli. Souhlas jako zákonný důvod zpracování osobních údajů se tak v pracovněprávních vztazích uplatní spíše výjimečně a spíše na případy, které se netýkají přímo výkonu práce (např. použití fotografie z teambuildingu v ročence).

Zpracovávané údaje musí být přesné, musí být zachována jejich integrita a důvěrnost. Zaměstnavatel má tedy povinnost je zabezpečit. Zabezpečení musí být provedeno vhodnými technicko-organizačními opatřeními. Vhodnost se posuzuje vzhledem k riziku neoprávněného či náhodného zničení, pozměnění, ztráty či zpřístupnění osobních údajů, stavu techniky, nákladům na provedení zabezpečení i povaze, rozsahu, kontextu a účelům zpracování osobních údajů.

Porušení zabezpečení musí zaměstnavatel hlásit Úřadu pro ochranu osobních údajů („**Úřad**"), ideálně do 72 hodin, ledaže je nepravděpodobné, že je toto porušení rizikem pro práva fyzických osob. Porušení zabezpečení může vést k pokutě dle GDPR a náhradě případné újmy. Porušením zabezpečení navíc může dojít i k porušení povinností dle jiných právních předpisů, např. OZ, neboť se může jednat o již zmiňované obchodní tajemství, či § 51 zákona č. 372/2011 Sb., o zdravotních službách, neboť může jít o data pacientů.

Pokud tedy zaměstnavatel poskytuje zaměstnancům pracovní notebook, telefon či jiná zařízení, musí zabezpečit osobní údaje uchovávané na těchto zařízeních proti neautorizovanému přístupu, změně a zničení. Vhodná technicko-organizační opatření zabezpečující tato data zahrnují např. vytvoření odděleného pracovního prostředí fungujícího přes VPN doplněného o vnitřní předpis a dohodu se zaměstnancem, které stanoví přesná pravidla nakládání se zařízením, ať již vlastním v režimu BYOD či zaměstnavatelovým. Pravidla musí pamatovat i na to, že ztráta zařízení či přístup k datům neoprávněnou osobou může být porušením zabezpečení osobních údajů a zaměstnavatel bude mít povinnost jej nahlásit Úřadu, přičemž ponese riziko sankce. Vnitřní předpis by tak měl v zásadě vždy a bez výjimky stanovit povinnost šifrovat data, neumožnit přístup k datům neoprávněným osobám a nenechávat zařízení odemknuté bez dozoru.

Zaměstnavatel má rovněž informační povinnost vůči zaměstnanci. Nejpozději k okamžiku získání osobních údajů musí zaměstnance informovat stručným, transparentním, srozumitelným a snadno přístupným způsobem minimálně o totožnosti a kontaktních údajích svých i svého zástupce a případného pověřence pro ochranu osobních údajů, o účelech zpracování, právním základu zpracování a případných oprávněných zájmech, na jejichž základě údaje zpracovává. Za jistých okolností je tato informační povinnost zaměstnavatele ještě rozšířena.

Závěr

Práva a povinnosti při nakládání s pracovními prostředky zaměstnavatele a BYOD nejsou kodifikována. Zákonodárce ukládá zaměstnavateli spíše mantinely, jak vztahy se zaměstnanci upravit. Zaměstnavatel by měl své povinnosti náležitě zvážit, odlišit od sebe případy výkonu kontroly

nad zařízením a nad daty jako takovými, kdo dané zařízení vlastní, jaká data obsahuje a jak je s nimi nakládáno a vhodným způsobem jednotlivé situace upravit ve vnitřním předpisu. Vnitřní předpis musí rovněž vhodně upravit otázku zabezpečení dat. Při tom všem nesmí dle § 305 odst. 1 ZP zaměstnanci ukládat povinnosti nad rámec zákona ani zkracovat jeho práva.

Při tvorbě těchto vnitřních předpisů tedy doporučujeme obrátit se na odborníky a předejít tak případným nesrovnalostem, které mohou vést ke sporům se zaměstnanci i veřejnoprávním sankcím. Stále totiž platí zásada *Vigilantibus iura scripta sunt* (Právo přeje bdělým).

Mgr. Karin Pomaizlová
JUDr. Markéta Cibulková, Ph.D.
Mgr. Radim Doležal

TaylorWessing

TaylorWessing e|n|w|c advokáti v.o.s.

U Prašné brány 1078/1
110 00 Praha 1

Tel.: +420 224 819 216
e-mail: k.pomaizlova@taylorwessing.com

---

[1] NS sp. zn. 21 Cdo 1009/98

[2] § 265 odst. 3 ZP

Další články:

- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Byznys a paragrafy, díl 32.: Konkurenční doložka
- Skryté ujednání v realitní smlouvě – zbytečná hra na schovávanou
- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026

- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu