PAVLA VACKOVÁ 9. PROSINCE 2020

BYOD & Ochrana osobních údajů & Home office

Identifikace rizik na poli ochrany osobních údajů při výkonu práce na vlastních zařízeních zaměstnanců – zejm. při práci z domova - a možnosti jejich mitigace

BYOD = PRÁCE ZAMĚSTNANCE NA VLASTNÍM ZAŘÍZENÍ

Filozofie: snížení nákladů na straně zaměstnavatele + zvýšení efektivity práce a flexibility zaměstnance

Zaměstnanec používá při výkonu práce typicky vlastní počítač, mobilní telefon, popř. tablet.

“Myšlenka je to dobrá, výsledky nejsou vždy dobré.”

Úskalí při implementaci BYOD politiky můžeme sledovat zejm. v těchto třech oblastech práva - problematika licencí zejm. SW, pracovně právní aspekty a ochrana osobních údajů.

ODPOVĚDNOST ZAMĚSTNAVATELE

Zaměstnavatel odpovídá za jednání svých zaměstnanců. “Právnickou osobu zavazuje protiprávní čin, kterého se při plnění svých úkolů dopustil člen voleného orgánu, zaměstnanec nebo jiný její zástupce vůči třetí osobě.”

Předpoklady pro dovození odpovědnosti zaměstnavatele za škodu způsobenou zaměstnancem třetí osobě (§ 167 OZ + použití pomocníka § 2914 OZ)

1) závislost zaměstnance na pokynech zaměstnavatele

2) zařazení do jeho organizační struktury

3) způsobení škody při výkonu svěřené činnosti

4) protiprávní a zaviněné jednání samotného pomocníka, případně jeho odpovědnost tam, kde zavinění není vyžadováno

Dle judikatury i když zaměstnanec jedná proti výslovnému zákazu zaměstnavatele avšak při této pracovní činnosti sleduje plnění pracovních úkolů, nepostrádá tato činnost zaměstnance věcný vztah k činnosti zaměstnavatele (21 Cdo 418/2011).

ODPOVĚDNOST ZAMĚSTNAVATELE II

Správce osobních údajů je povinen zavést vhodná technická a organizací opatření, aby zajistil a byl schopen doložit , že zpracování OÚ je prováděno v souladu s GDPR. (čl. 24 dost. 1 GDPR)

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

- nápravná opatření: čl. 58 odst. 2 písm. a) až h) a j) GDPR
- správní pokuty “Ukládání správních pokut musí být účinné, přiměřené, ale zároveň odrazující. “ do výše 10 000 000 eur (nebo až do 2 % celkového ročního celosvětového obratu, jde-li o podnik) nebo do výše 20 000 000 eur (nebo až do 4 % celkového ročního celosvětového obratu, jde-li o podnik).

Polehčující a přitěžující okolnosti jsou vyjmenovány v čl. 83 odst. 2 písm. a) až k) GDPR dle povahy, závažnosti a délky trvání porušení s přihlédnutím k povaze, rozsahu a účelu zpracování, kategorií údajů a počtu dotčených subjektů údajů, zda se jednalo o úmyslné či nedbalostní porušení, ap.

OPATŘENÍ VŮČI SUBJEKTU VEŘEJNÉ SPRÁVY

Zákon č. 110/2019 Sb., o zpracování osobních údajů, vylučuje z udílení správních pokut orgány veřejné moci a veřejné subjekty. - ÚOOÚ upustí od uložení pokuty, ale ukládá nápravná opatření

V ČEM SPOČÍVÁ HLAVNÍ RIZIKO BYOD POLITIKY?

- Mix dvou typů údajů na jednom zařízení - osobní údaje zaměstnance a zaměstnavatele
  - vlastní citlivé údaje (typicky OÚ zaměstnanců, ale i obchodní tajemství) a OÚ třetích osob (typicky zákazník)
- hrozí ztráta, únik nebo zneužití osobních údajů “Největším bezpečnostním rizikem je zaměstnanec.”
  - např. soukromá aplikace získá přístup ke kontaktům z pracovního emailu
- hrozí riziko nežádoucího zásahu do osobních údajů zaměstnance “Cesta do pekel je dlážděna dobrými úmysly.”
  - např. geolokační systémy sledující pohyb zařízení, ale tím i zaměstnance

MITIGACE RIZIK - JAK NA TO?

POSOUZENÍ VLIVU ZPRACOVÁNÍ NA OCHRANU OSOBNÍCH ÚDAJŮ čl. 35 GDPR

1. Identifikovat typy zpracování OÚ: specifický účel, kategorie zpracovávaných osobních údajů, veřejnost zpracování, jeho částí nebo výstupů ze zpracování zakládaného navrhovanou regulací správce a lhůty pro uchování osobních údajů
2. Dopady zpracování na soukromí subjektu údajů - resp. popis zásahu
3. Identifikace a popis kanálů a uzlů kudy OÚ tečou + specifikace účelu dle čl. 5 GDPR
4. Přiřazení rizik pro OÚ v rámci jednotlivých kanálů
5. K rizikům se přiřadí protiopatření
6. Posouzení - jsou opatření dostatečná, popř. co je třeba zlepšit

VÝSLEDEK POSOUZENÍ VLIVŮ NA OÚ

VNITŘNÍ PŘEDPIS: obecná pravidla pro zacházení s OÚ

Kategorizace osobních údajů a dat - klasifikace dle standardů např. DIN 66399

Úprava přístupových práv (kdo, kdy, kam), pravidla pro tvorbu hesel

Pravidla chování pro případ bezpečnostního incidentu (okamžité hlášení incidentu, okamžité hlášení ztráty)

Pravidla emailové komunikace, videokonferencí

Pravidla pro instalaci SW a aktualizací

Fyzické zabezpečení dat

Pravidla monitorování zaměstnance, přístupu k polohovým údajům

Pravidla pro home office

TECHNICKÁ OPATŘENÍ

Oddělení soukromých a pracovních dat (např. dělení disku)

Zásadně využití vzdáleného připojení - VPN

Zaměstnanec má vždy aktuální antivirový program

Nastavení mechanismu pro přepínání mezi pracovním a soukromým využitím zařízení (např. různost uživatelských profilů)

Omezení přístupu k pracovním datům (např. časové ohraničení)

Možnost výmazu firemních dat při ztrátě zařízení

NÁHRADA NÁKLADŮ

§ 190 ZP “Sjedná-li zaměstnavatel, popřípadě vnitřním předpisem stanoví nebo individuálně písemně určí podmínky, výši a způsob poskytnutí náhrad za opotřebení vlastního nářadí, zařízení nebo jiných předmětů potřebných k výkonu práce zaměstnance, poskytuje mu tuto náhradu za dohodnutých, stanovených nebo určených podmínek.”

- možný postih od inspekce práce až do výše 200.000 Kč

HOME OFFICE = PRÁCE Z DOMOVA

- nelze ji nařídit zaměstnavatelem
- nejlépe individuální dohoda s každým zaměstnancem + úprava pravidel ve vnitřním předpise

např. pravidla pro střídání se v kanceláři

- zaměstnanci náleží náhrada nákladů (lze upravit vnitřním předpisem, stanovit paušál)
- pracovní dobu určuje i nadále zaměstnavatel - pokud se nejedná o zaměstnance v režimu §317 ZP
- pracovní místo doma by mělo splňovat požadavky dle pravidel BOZP - zaměstnanec by měl být speciálně poučen a potvrdit, že jeho domov tyto nároky splňuje

HOME OFFICE: CO JE TŘEBA NASTAVIT?

STANOVENÍ ZÁKLADNÍCH PODMÍNEK, BEZ JEJICHŽ NAPLNĚNÍ NEBUDE UMOŽNĚNA HOME-OFFICE / BYOD

Kde? Vnitřní předpis (samostatná kapitola - home office)

1. **vymezení pracovních pozic, které ano / ne**
2. **rozvržení pracovní doby - kdy bude zaměstnanec k dispozici, pauza**
3. **pravidla BOZP - nastavení pravidel jako v zaměstnání**

   Pozor: §101 odst. 6 ZP “Náklady spojené se zajišťováním bezpečnosti a ochrany zdraví při práci je povinen hradit zaměstnavatel; tyto náklady nesmějí být přenášeny přímo ani nepřímo na zaměstnance.”
4. **síťová bezpečnost - ideálně šifrované VPN zaměstnavatele**
5. **pravidla komunikace mezi zaměstnanci - zákaz použití jakýchkoli soukromých kanálů (FB Messenger, apod.)**
6. **fyzická bezpečnost dat: pracovní místo, nakládání s dokumenty a zařízeními**

FYZICKÁ BEZPEČNOST DAT - PRAVIDLA PRACOVNÍHO MÍSTA

1. ideálně samostatný uzamykatelný pokoj, pokud to není možné vyčlenit oddělený pracovní kout
2. pracovat výhradně ze soukromých prostor zaměstnance (ne park, kavárna) - pozor na práci na zahradě
3. clean-desk policy
4. viditelnost do bytu (okenní folie, záclony, závěsy, zavřená okna)
5. odhlášení z pracovního prostředí kdykoliv na delší dobu fyzicky opustí pracovní stůl a není v bytě sám

6. telefonní hovory a videokonference zásadně ne před dalšími členy domácnosti

FYZICKÁ BEZPEČNOST DAT - NAKLÁDÁNÍ S DOKUMENTY/ZAŘÍZENÍMI

1. dokumenty jsou přenášeny v deskách, cestou domů nepodstupovat zbytečná rizika (nakupování, hospoda)
2. dokumenty nenechávat volně na stole, ideálně uzamykatelná skříň / šuple + clean desk policy
3. skartovat - pokud nelze doma, pak v práci
4. vyloučit rizikové elementy - děti, domácí mazlíčci

OPATŘENÍ VE VZTAHU K ZAMĚSTNANCŮM

1. úvodní prověření každého vlastního HW používaného zaměstnanci se souhlasem zaměstnance
2. pravidelná aktualizace SW
3. školení zaměstnanců
4. absolutní zákaz stahování pracovních dokumentů “na céčko” když jsou problémy s připojením, zákaz přeposílání na soukromý email
5. písemný závazek zaměstnance, že byl s pravidly BYOD a HO seznámen a že je bude dodržovat - pravidla formulovat PREGNANTNĚ
6. NEUPLATŇOVAT, co nelze: pokud zaměstnanec nemá podmínky pro HO nebo využití vlastního zařízení, pak pracuje z kanceláře / na zařízení zaměstnavatele

DĚKUJI ZA POZORNOST!

Mgr. Bc. Pavla Vacková

Advokátka, ev. č. ČAK 18531

Adresa: Varšavská 714/38, 120 00 Praha 2

Email: vackova@exiure.cz

www: www.advokat-vackova.cz ww.exiure.cz

Telefon /WApp: +420 732 125 473

微信： baifen_liska

EXIURE