31. 1. 2018

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

BYOD z perspektivy GDPR

Koncept BYOD[1] představuje progresivní a svým způsobem velmi pragmatický model zaměstnanecké politiky, který zvyšuje pracovní komfort zaměstnanců. Podstatou tohoto konceptu je umožnit zaměstnancům výkon práce na vlastních zařízeních, typicky noteboocích, tabletech či chytrých telefonech.

Filozofie tohoto konceptu je v zásadě velmi prostá a s trochou fantazie by se dala opsat rčením „ševče, drž se svého kopyta," když vychází z premisy, že je-li zaměstnanec uvyklý pracovat s určitým zařízením, operačním systémem, atp. bude jeho práce na tomto zařízení aj. vykonávána nutně efektivněji než-li na zařízení, které pracuje a je obsluhováno jiným způsobem.

Tento model umožňuje snižovat náklady zaměstnavatele na vybavení a je třeba zdůraznit, že jím je zaručena i vyšší flexibilta zaměstnance, jeho dostižitelnost a operativnost při řešení či přípravě řešení úkolů. To vše s benefitem zajištění komfortu dotčeného zaměstnance jak co do znalosti uživatelského prostředí konkrétního zařízení, tak co do kvantity obsluhovaných zařízení. (Koneckonců podněty pro zavedení BYOD vychází převážně z řad zaměstnanců, když zaměstnanci k užívání jimi „osvojených" zařízení přirozeně - někdy nekontrolovaně - inklinují.)

Pro názornost uveďmě jednoduchý obecný příklad: pokud je zaměstnanec omezen při výkonu své činnosti na „pracovní" PC nacházející se na určeném pracovišti (tzv. desk-based employees), nemůže tuto činnost vykonávat z jiného místa. Byť je tedy po něm vyžadováno splnění jakkoliv jednoduchého jakkoliv časově nenáročného pracovního úkolu, zaměstnanec se musí dopravit do místa obvyklého výkonu práce. Také v případě cesty na obchodní jednání se nemůže zaměstnanec operativně připravovat. Tato potřeba může mít za následek také například přenos dokumentů na osobní zařízení bez vědomí zaměstnavatele. Či příklad jiný: pokud je zaměstnanci svěřen „firemní" mobilní telefon, je zde vyšší pravděpodobnost jeho nezastižitelnosti, nehodlá-li mít při sobě permanentně obě svá mobilní zařízení či na úkor vlastních potřeb bude mít při sobě pouze zařízení zaměstnanecké, což jde zcela proti duchu doby, kdy jsou veškerá zařízení integrována ve stále menší a kompaktnější celky (viz př. telefonování skrze hodinky).

Obecně lze pak také konstatovat, že koncept BYOD je jen dalším projevem fenoménu prorůstání soukromého a pracovního života, jeho dalším kvalitativním stupněm typickým zejména pro sektor služeb.

Implementace konceptu však není v žádném případě „růžová". Pomineme-li problémy, které sebou zavedení této politiky přináší z hlediska pracovního, autorského či daňového práva, není jeho zavedení bez překážek ani z hlediska evropského Obecného nařízení o ochraně osobních údajů –

“General Data Protection Regulation” (dále jen „GDPR“). Z tohoto hlediska dochází k prolínání dvou pomyslných„světů“ - světa zaměstnavatele a světa zaměstnance.

Zaměstnavatel se zejména bude snažit eliminovat možnost neoprávněného úniku a zneužití či ztráty jím chráněných obchodních, resp. osobních dat, informací o zaměstnancích, atp. v jakémkoli myslitelném rozsahu (takový únik dat může vyplynout například ze zdánlivě nevinného zapůjčení tabletu „na hraní“ dítěti). Jednoduše řečeno: vzdálený přístup k datům společnosti ze soukromého zařízení zaměstnance představuje pro zaměstnavatele bezpečnostní riziko (i z hlediska GDPR), což bývá vyvažováno monitoringem těchto zařízení ze strany zaměstnavatele, eventuálně stopováním zařízení pro případ jeho ztráty.

Taková opatření pak představují zásah do „světa“ zaměstnance (zejména z hlediska GDPR), když tento se může obávat nepřiměřeného zásahu do svého soukromí a neoprávněného zpracování osobních údajů (například přístupu zaměstnavatele k účtům, údajům o zdravotním stavu, fotografiím, videím, kontaktům, polohovým údajům, aj.) a popřípadě také ztráty těchto osobních dat (např. v důsledku bezpečnostního skenování zařízení za účelem odhalení malwaru).

Jak však tyto rozpory v souladu s GDPR vyřešit?

Odrazovým můstkem je spolupráce se samotnými zaměstnanci. Zaměstnanci si musí být vědomi nabízeného benefitu a odpovědnosti zaměstnavatele. Fungující systém je pak průsečíkem obojího. Zaměstnanci musí být patřičně proškoleni o zásadách, cílech a smyslu nařízení GDPR, musí pochopit hrozící konsekvence, ale také musí jasně artikulovat své požadavky stran přístupnosti a obsluhy zařízení event. softwaru. Zaměstnavatel musí vyjít vstříc zaměstnancům v rozsahu naplnění požadavků vycházejících ze zásad nařízení GDPR, zejména minimalizovat množství operací zpracování osobních údajů ve vztahu k vymezenému účelu a důvodu zpracování. Ve zkratce: Zaměstnanci a zaměstnavatel musí být na jedné lodi.

Výstupy tohoto procesu by pak mělo být Posouzení vlivu na ochranu osobních údajů – “Data Protection Impact Assessment”, tj. DPIA analýza zohledňující nutnost zavedení určitých technolgií, posuzující soulad výsledného zpracování osobních údajů v souladu se zásadami proporcionality a subsidiarity, stanovivší a hodnotící potenciální a vhodná opatření k minimalizaci zpracování osobních údajů a předcházení jejich zneužití.

Dalším výstupem by měl být minimálně interní předpis zaměstnavatele, který bude odrážet přijatou BYOD politiku ale také vysvětlovat ochranná opatření zaměstnavatele před únikem jím chráněných dat. Ta by měla zahrnovat zejména následující:

- stanovit mechanismy, které umožní oddělit pracovní data od soukromých (např. delění disku)
- stanovit mechanismy, jak může zaměstnanec „přepínat“ mezi obchodním a soukromým využitím zařízení (například různost uživatelských profilů), aby měli zaměstnanci možnost ochránit soukromé užití zařízení před jakýmkoliv sledováním ze strany zaměstnavatele
- stanovit kdo a z jakých zařízení či aplikací bude mít přístup ke specifikovaným datům vč. stanovení a vysvětlení mechanismů detekce přístupů
- zakotvit mechanismy blokování dat (např. nemožnost přepisu, sandboxing), popř. monitorovat jejich sdílení, umožňovat přístup pod logem, heslovat některé soubory a složky
- určit podporovaná zařízení, zavazovat k pravidelným aktualizacím užívaných aplikací
- stanovit bližší pravidla, vypracovat pokyny pro přístup k firemním datům (vč. například časového ohraničení), resp. užívání zařízení k pracovním účelům
- stanovit bližší pravidla monitorování ze strany zaměstnavatele (například za jakých podmínek

bude zaměstnavateli umožněn servis pro účely odhalení malwaru), tyto vysvětlovat včetně jejich důsledků pro zaměstnance
- vysvětlovat způsob ochrany osobních údajů zaměstnanců, kdo k nim, kdy a za jakých okolností bude mít přístup (např. přístup k polohovým údajům pouze v případě ztráty zařízení)
- zavazovat zaměstnavatele k zajištění školení zaměstnanců a pravidelné revizi fungování a plnění účelu systému, určit kontaktní osobu s níž je možné řešit nejasnosti, stížnosti, atj.

Závěr

BYOD představuje velmi praktický a pozvolna stále více se prosazující model vztahu mezi zaměstnavatelem a zaměstnancem, který se v praxi realizuje v jakési šedé, „nepřiznané“ zóně. S nabytím účinnosti nařízení GDPR se však tato forma spolupráce bez promýšlení a přijetí patřičných opatření stane pro zaměstnavatele velmi rizikovou.

Jakkoliv nelze (bez znalosti konkrétních potřeb každé společnosti resp. organizace) stanovit vyčerpávající a jednoznačný návod pro implementaci BYOD, lze s jistotou uzavřít, že alfou a omegou zavedení tohoto konceptu je zajištění toho, aby byla tato implementace nanejvýše komplexní, citlivě reflektovala a naplňovala cíle GDPR.

Mgr. Filip Losert

Advokátní kancelář JELÍNEK & Partneři s.r.o.

Pardubice - Dražkovice 181
533 33 Pardubice - Dražkovice

Velké náměstí 1
500 03 Hradec Králové

Truhlářská 1108/3
110 00 Praha 1

Tel.: +420 466 310 691
Fax: +420 466 310 691
gsm: +420 724 794 986
e-mail: advokati@advokatijelinek.cz

_____
[1] Bring Your Own Device neboli česky „přines své vlastní zařízení“.

Další články:

- Evropská unie mění pravidla plateb: více odpovědnosti, intenzivnější zpracování dat, více kontrol

- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Novinky z české a evropské regulace finančních institucí za měsíc květen 2026
- Sport versus EU – aktuální sportovní kauzy rozhodované Soudním dvorem EU
- Postavení finančního arbitra v kontextu nařízení Brusel I bis - Funkční pojetí „soudu“, osvědčení podle čl. 53 a možnost výkonu nálezu v jiných členských státech EU
- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Novinky z české a evropské regulace finančních institucí za měsíc duben 2026
- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Novinky z české a evropské regulace finančních institucí za měsíc březen 2026