Privacy Flash

březen 2020

Home office aneb na co si dávat pozor z pohledu zaměstnavatele

Možná jste již měli možnost přečíst si naše newslettery, týkající se vyhlášeného nouzového stavu nebo shrnující dopady pandemie COVID-19 na zaměstnavatele. Jedním z mnoha efektů této pandemie je masový přesun práceschopného obyvatelstva na tzv. home office – práci z domova. Jakkoliv toto téma může být pro někoho samozřejmé a pro některé provozy naopak nepředstavitelné, reálně zažíváme bezprecedentní využívání tohoto způsobu práce. Mnoho z Vás tak nyní řeší kromě technického zajištění i právní problémy související s prací z domova, informování o zdravotním stavu zaměstnanců za účelem organizace práce, ukládání dat do cloudu a vytvoření virtuálního pracoviště. Navíc mnohé IT společnosti zareagovaly na novou situaci bezplatnou nabídkou softwarových řešení pro videokonference.

Při řešení organizace práce nezřídka překotným způsobem (což je naprosto pochopitelné vzhledem k obdobnému způsobu zavádění nouzových opatření na vládní úrovni) už ale společnosti pozapomínají na aspekty ochrany osobních údajů, které spolu s pandemií nepřestaly platit. I za takto mimořádné situace je nezbytné dodržovat zákony, včetně GDPR, nechceme-li se po překonání nynější krize probudit do ještě větších strastí, než které působí přímo či nepřímo řádící virus SARS-CoV-2. To potvrdil i Evropský sbor pro ochranu osobních údajů ve svém prohlášení.[1]

Pojďme se společně podívat na devět praktických doporučení, jak zvládat home office bezpečně.

Problém č. 1: Seznamy zaměstnanců v karanténě, popř. nakažených zaměstnanců

Zpracovávání informací o zdravotním stavu zaměstnance představuje zpracování tzv. zvláštní kategorie osobních údajů dle čl. 9 GDPR. Zaměstnavatel je oprávněný takovouto informaci zpracovávat za účelem plnění povinností vyplývajících z pracovního práva a práva sociálního zabezpečení [čl. 9 odst. 2 písm. b) GDPR]. Navíc dle ustanovení § 101 zákoníku práce má zaměstnavatel povinnost zajistit bezpečnost a ochranu zdraví svých zaměstnanců. Tudíž je možné vést evidenci zaměstnanců s příznaky koronaviru anebo zaměstnanců, kteří po návratu z rizikových oblastí jsou v karanténě. Zaměstnavatel však nesmí zveřejňovat seznamy těchto zaměstnanců, může pouze informovat o celkovém počtu zaměstnanců v karanténě.

Problém č. 2: Testovací verze a bezúplatné poskytnutí programů na videokonference, sdílené pracoviště, cloudová řešení

Dříve než společnost využije nabídky IT firem, měla by zvážit několik aspektů: (i) jak je celé navrhované řešení koncipováno: kde jsou servery, kam se ukládají informace, kdo má přístup k datům a odkud firmy zajišťují technickou podporu – často jsou uložiště v cloudu a servery po celém světě a přístup je zajišťován společnostmi mimo EU. Firma, která využívá takovéto řešení, je pak odpovědná za zajištění legálnosti přeshraničního přenosu osobních údajů, aniž by často věděla, že k němu dochází; (ii) připojení do videokonference – mělo by být možné pouze po připojení přes VPN (Virtual Private Network), obzvláště mají-li být součástí rozhovorů důvěrné informace, tím se zajistí zabezpečení přenosu dat sdílených během konference; (iii) mělo by být znemožněno nahrávat soubory do dočasně používaného programu na videokonference, aniž byste si ověřili, kde přesně jsou údaje uchovávány a kdo k nim má přístup; (iv) to samé se týká případných nahrávek videokonferencí.

Problém č. 3: Nahrávání videokonferencí

Mezi základní principy stanovené v čl. 5 GDPR patří transparence. Tento princip vyžaduje, aby účastníci telekonference byli předem informování, nejlépe v pozvánce k ní, že hovor se bude nahrávat. Pokud některý účastník chce položit dotaz, ale nechce být u toho nahrávaný, měl by mít možnost dotaz položit předem formou e-mailu anebo chatu. Také je nezbytné na začátku videokonference informovat všechny účastníky o nahrávání. Kromě toho je nezbytné stanovit pravidla (i) jaké telekonference je možné nahrávat a za jakým účelem, (ii) kam se budou nahrávky ukládat, (iii) kdo k nim bude mít přístup a (iv) jak dlouho se budou uchovávat.

Problém č. 4: Jak sdílet dokumenty a složky

Zaměstnanci potřebují sdílet často objemné soubory dat. Za účelem zabezpečení dat, nejen osobních, ale i obchodních důvěrných informací, musí být nastaven způsob, jak soubory sdílet a vyvarovat se sdílení formou bezúplatných uložišť, která nejsou dostatečně zabezpečena. Doporučené jsou sdílené disky, popř. cloudová řešení s omezeným přístupem (s nutností přihlášení se svým loginem a heslem). Samotné zaslání pravidel e-mailem by bylo postačující za předpokladu, že máme 100% jistotu, že taková pravidla budou zaměstnanci dodržovat, což obvykle chybí. Předejít neoprávněnému sdílení lze pouze tak, že zaměstnanec se na stránky uložišť nedostane, tj. vybrané webové stránky budou na tzv. blacklistu.

Problém č. 5: Stěhování šanonů

Práce může vyžadovat práci s fyzickými dokumenty. Zaměstnanci by měli minimalizovat přemísťování papírových dokumentů. Když už je nezbytné si domů nějaké dokumenty odnést, zaměstnanec musí s dokumenty

[1] https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en.

Privacy Flash

březen 2020

obsahujícími osobní údaje nakládat obezřetně, aby nedošlo k jejich ztrátě v MHD anebo si z nich dítě neudělalo leporelo. Je vždy na zvážení, jestli není bezpečnější práci rychle udělat na pracovišti, a vyhnout se tak riziku ztráty dokumentů a tím porušení čl. 32 GDPR.

Problém č. 6: Kontrola zaměstnance na home office

Zaměstnavatel má legitimní důvod kontroly zaměstnance na home office, včetně přiděleného agenturního zaměstnance. Vedle kontroly prostřednictvím telefonu může využívat různé softwary, které sledují čas, jaký zaměstnanec stráví u počítače, anebo chattery, které evidují, jak dlouho je uživatel již neaktivní. Za účelem naplnění principu transparentnosti zaměstnavatel musí zaměstnance o kontrole informovat. Není možné naistalovat zaměstnancům do počítače software, který monitoruje čas strávený u počítače, aniž by o tom věděli – naopak zaměstnancům musí být naprosto zřejmé, jakým způsobem je jejich pracovní doba evidovaná, když to není obvyklý příchod a odchod z pracoviště. Současně je třeba se vyvarovat unáhleným závěrům při použití těchto automatických metod – pokud povaha práce zaměstnance nespočívá v permanentní práci s počítačem, ale může například studovat písemné podklady, pak neaktivita chatu, resp. vypnutý laptop, nemůže být podkladem pro automatickou výtku, že daný zaměstnanec nepracuje (na rozdíl třeba od pracovníka call centra, kde je takováto souvislost naopak zřejmá). Také je doporučené stanovit, kdo bude oprávněný ke kontrole zaměstnanců (pověřený zaměstnanec) a jaká opatření může vůči ostatním zaměstnancům přijmout. Bez dostatečného informování zaměstnanců nelze informaci o neplnění pracovních úkolů použít ani za účelem nápravných opatření vůči zaměstnanci (např. výtka).

Problém č. 7: Phishing

Bohužel ani mimořádná situace nevede ke snížení phishingových útoků. Naopak, s poklesem ekonomických aktivit a potenciálnímu snížení množství pracovních e-mailů zaměstnanci spíše kliknou na lákavý odkaz v e-mailu anebo se přihlásí přes falešný portál. I Úřad pro ochranu osobních údajů nabádá společnosti k opatrnosti.[2] Zaměstnavatelé by měli apelovat u zaměstnanců na zvýšenou obezřetnost a zvýšit ochranu formou firewallů, aby snížili množství phishingových e-mailů, které se dostanou až k zaměstnanci. Pokud má společnost zavedený systém e-learningu, může být toto období s nižším vytížením využito právě ke vzdělávání, včetně počítačové bezpečnosti.

Problém č. 8: Bezpečnostní incident

Ztráta šanonu nebo neoprávněný přístup k osobním údajům v případě vydařeného phishingu může naplnit definici porušení zabezpečení osobních údajů dle čl. 33 GDPR. V takovémto případě je zaměstnavatel povinen informovat Úřad pro ochranu osobních údajů ve lhůtě 72 hodin od zjištění incidentu, anebo od okamžiku, kdy k němu došlo. Vyplatí se připomenout všem zaměstnancům pravidla bezpečného nakládání s (nejen osobními) údaji, neboť rozptýlená práce mimo objekty zaměstnavatele a obvyklý zabezpečený síťový perimetr zvyšuje jak riziko samotného incidentu, tak i jeho pozdějšího odhalení. Zaměstnanci by se současně neměli bát informovat zaměstnavatele o možném incidentu a ten by incident měl konzultovat se svým pověřencem anebo právníkem.

Problém č. 9: Sankce

Stanovení pravidel bez sankcí bývá neúčinné. Doporučeným řešením je stanovit pravidla pro práci z domova ve formě vnitřního předpisu dle ustanovení §305, resp. 306 zákoníku práce, který stanoví i případné sankce za nedodržení. Směrnice musí být šitá na míru Vaší organizaci a Vašim zaměstnancům, např. v případě operátorů nezapomeňte ve směrnici uvést, že při vyřizování hovorů by měli být v samostatné místnosti bez rodinných příslušníků, vytištěné dokumenty by měly být zaneseny zpět do firmy k bezpečné likvidaci, jakmile to bude možné, uzamykání obrazovky počítače by mělo být samozřejmostí i doma.

---

[2] *Dne 19. 3. 2020 Úřad pro ochranu osobních údajů sdílel tento článek: https://www.novinky.cz/komercni-clanky/clanek/podvodne-e-maily-zneuzivaji-aktualni-kauzy-cilem-jsou-vase-data-40316964.*

Autoři:
Robert Nešpůrek | *Partner*
Richard Otevřel | *Counsel*
Jitka Soukupová Ivančíková | *Právní expert (FairData)*



HAVEL & PARTNERS

ÚSPĚCH SPOJUJE

Náš tým

220 právníků a daňových poradců | **400** spolupracovníků

Naši klienti

2 000 klientů | **100** největších světových společností z Fortune 500
50 společností z Czech Top 100 | **7** společností z Czech Top 10

Mezinárodní dosah

Právní poradenství
ve více než **90** zemích světa
ve **12** světových jazycích
až **70 %** případů zahrnuje mezinárodní prvek

www.havelpartners.cz

PRAHA
Florentinum, recepce A
Na Florenci 2116/15
110 00 Praha 1
Česká republika
Tel.: +420 255 000 111

BRNO
Titanium Business Complex
Nové sady 996/25
602 00 Brno
Česká republika
Tel.: +420 545 423 420

BRATISLAVA
Centrum Zuckermandel
Žižkova 7803/9
811 02 Bratislava
Slovenská republika
Tel.: +421 232 113 900

PLZEŇ
Nepomucká 144
326 00 Plzeň
Česká republika
Tel.: +420 371 005 320

OLOMOUC
Salmův palác
Horní náměstí 371/1
779 00 Olomouc
Česká republika
Tel.: +420 581 000 310

OSTRAVA
Smetanovo náměstí 979/2
702 00 Moravská Ostrava a Přívoz
Česká republika
Tel.: +420 255 000 111