TaylorWessing

# GDPR a COVID-19

Jak uvedl Evropský sbor pro ochranu osobních údajů, pravidla ochrany osobních údajů včetně GDPR nebrání opatřením přijatým v boji proti pandemii koronaviru, ale i v těchto výjimečných časech musí osoby a organizace, včetně orgánů veřejné správy, které shromažďují a zpracovávají osobní údaje, zajistit ochranu osobních údajů jednotlivců. Jakákoliv opatření přijatá v souvislosti s nouzovým stavem, ale i nadále pokračující soukromoprávní aktivity včetně dobročinných projektů, musí respektovat zásady ochrany soukromí jednotlivců a nesmí být nevratné. Nouzová situace může legitimizovat omezení svobod občanů, ale jen pokud jsou tato omezení přiměřená a omezená na dobu nouze a pokud jsou zpracovávané osobní údaje užity za účelem prevence šíření infekce koronaviru.

## Před zpracováním osobních údajů

Ve světle výše uvedeného je nutné zdůraznit důležitost zásad zpracování osobních údajů, stanovených GDPR. Jedná se zejména o zásadu **transparentnosti**, která vyžaduje důsledné a přehledné informování občanů o tom, jak je s jejich osobními údaji nakládáno, a dále pak o zásady **minimalizace zpracování a účelového omezení** – s osobními údaji je možné provádět pouze takové operace, které jsou nezbytně nutné k dosažení velmi úzce stanoveného účelu, kterým je např. zjištění možného ohniska nákazy a informací o šíření této nákazy, a musí být implementováno časové omezení takového zpracování.

Vždy je proto nutné shromažďovat osobní údaje transparentně, dotčené osoby informovat o tom, kdo a za jakým účelem bude jejich osobní údaje zpracovávat, po jak dlouhou dobu a na základě jakého právního důvodu. Tyto informace by měly být snadno dostupné, ideální je umístit odkaz na viditelné místo, například v případě registrace do e-shopu nebo na akci by měl stačit jeden klik. Dále by jejich formulace měla být přizpůsobena tomu, komu je určena (zejména pokud jsou uživatelé dětmi, v českém prostředí osoby mladší 15 let). Mezi nezbytné informace patří mimo výše uvedeného například i specifikace konkrétního oprávněného zájmu, na kterou se často zapomíná, a údaje o osobách, kterým hodláte osobní údaje zpřístupnit. Někteří správci také předávají osobní údaje do zemí mimo EU či provádějí automatizované individuální rozhodování – i o tom je nutné subjekty údajů poučit.

Povinnosti správce nicméně nezačínají informací subjektu údajů, ale jdou ještě dále před zahájení zpracování. Je nutné zejména věnovat náležitou péči návrhu procesu zpracování osobních údajů a již při jeho vytváření identifikovat jednoznačný účel a k němu odpovídající právní základ (ať se již bude jednat o plnění zákonné či smluvní povinnosti, oprávněný zájem nebo souhlas). Při tom je třeba zohlednit zásady tzv. záměrné a standardní ochrany osobních údajů. Tedy navrhovat proces zpracování tak, aby představoval co možná nejmenší zásah do soukromí subjektu (potřeboval ke svému fungování minimum osobních údajů). V případě jeho možné škálovatelnosti platí, že je na subjektu, zda zvolí takovou podobu procesu zpracování, která pracuje s větším množstvím osobních údajů.

## Během zpracování osobních údajů

I během nouzového stavu je potřeba myslet na dodržování povinnosti odpovídat na žádosti ohledně uplatnění práv subjektů údajů dle GDPR a upravit interní procesy tak, aby tato povinnost byla dodržena. Lhůta pro odpověď na žádost s uvedením přijatých opatření je 1 měsíc od obdržení takové žádosti. Tuto lhůtu je možné ve výjimečných situacích (pod kterou by se pandemie COVID-19 dala zařadit) prodloužit, avšak maximálně o 2 měsíce. Ale i v tomto případě je nutné na žádosti reagovat a vyrozumět žadatele do 1 měsíce od podání žádosti, že dojde k prodlení s jejím vyřízením a jako důvod uvést např. omezení provozu společnosti jako důsledek koronaviru.

Dále je třeba detekovat a hlásit porušení zabezpečení osobních údajů. Na této povinnosti se během trvání nouzového stavu nic nemění, stejně jako na povinnosti zabezpečit odpovídajícím způsobem celé zpracování, aby k incidentům nedocházelo. Lze si nicméně představit, že (obdobně jako v případě prodloužení reakce na žádost subjektu) bude možné opožděné hlášení incidentu Úřadu odůvodnit nedostatečnými personálními kapacitami správce.

Co však nelze omezit, je povinnost vést odpovídající dokumentaci o zpracování. Ta vyplývá ze zásady odpovědnosti, která stanoví, že správce odpovídá za dodržení pravidel dle GDPR a musí být schopen to prokázat. Stále je tak třeba vést záznamy o zpracování, evidovat žádosti subjektů, incidenty a jejich vyřízení, mít dokumentovány balanční testy oprávněných zájmů a bezpečnostní opatření a další.

Může se stát, že se na vás obrátí další subjekt (zejména státní orgán) s žádostí o předání dat za účelem boje proti šíření nákazy. V tomto ohledu lze jen doporučit postupovat uvážlivě a v případě nejasností si nechat vše vysvětlit – současná situace totiž nahrává podvodným žádostem o vydání osobních údajů, a je třeba pamatovat na to, že vydání osobních údajů neoprávněné osobě či v nadměrné míře nebo pro nelegitimní účel není možné odůvodnit současnou situací a vedlo by k porušení zabezpečení osobních údajů, a koneckonců ani státní orgány nemají právo na vše.

Níže rozpracováváme některé situace, které jsou v současné situaci více frekventované a správci se častěji potýkají s jejich právními aspekty, jako je práce z domova, prevence nákazy na pracovišti nebo zpracování osobních údajů v souvislosti s provozem e-shopu či pořádáním webinářů a dobročinných sbírek.

## Práce z domova

Řada firem umožnila svým zaměstnancům pracovat z domova a připojit se k firemním systémům na dálku. Pokud zaměstnanec nemá firemní notebook, který je vybaven bezpečným připojením do systémů zaměstnavatele, může to být problém. V zásadě i při práci z domova bychom měli dbát na to, aby data, která na počítači zpracováváme včetně osobních údajů, byla zabezpečena stejně jako při práci ze zaměstnání. Vedle softwarového zabezpečení, antiviru, jde i o robustní heslo a nesdílení pracovního počítače s členy rodiny. V období jako je toto, se počet kybernetických útoků zvyšuje. Při zcizení počítače může dojít k narušení důvěrnosti a integrity dat, která jsou uložena v jeho paměti. Pokud si lidé doma tisknout pracovní dokumentaci v zásadě by měli dbát na to, aby byla zachována i důvěrnost všech vytištěných pracovních dokumentů, ať už obsahují osobní údaje či nikoliv. Pokud dojde ke zcizení počítače, telefonu nebo vytištěných dokumentů, které obsahují osobní údaje, i toto představuje bezpečnostní incident, který musí zaměstnanec hlásit zaměstnavateli, který je pak nutno

nahlásit Úřadu pro ochranu osobních údajů. Proto při tištění dokumentů v domácnosti je rovněž nutné zajistit jejich bezpečné uschování nebo skartaci. Rovněž je na místě v této souvislosti zmínit, že podle zákoníku práce zaměstnavatel nemá právo monitorovat výkon práce zaměstnanců z domova prostřednictvím různých softwarových nástrojů, aby např. kontroloval čas strávený prací na počítači. Výkon práce lze samozřejmě kontrolovat, např. kontrolou splněných úkolů, nikoliv však pomocí čidel nebo aplikace na monitorování činnosti zaměstnance na PC.

## Prevence nákazy na pracovišti

Zákoník práce ukládá zaměstnavatelům, aby zajistili bezpečnost a ochranu zdraví zaměstnanců při práci s ohledem na rizika možného ohrožení jejich života a zdraví, která se týkají výkonu práce. Tato povinnost se vztahuje i na všechny fyzické osoby, které se s jeho vědomím zdržují na jeho pracovištích, tzn. i na návštěvníky, dodavatele, obchodní partnery a zákazníky.

Může jít např. o evidenci osob pohybujících se v prostorech organizace, záznamy o tom, koho a kdy navštívily a jejich kontaktní údaje. Tyto údaje mohou být následně využity příslušnou hygienickou stanicí při trasování nakažené osoby a osob, které se potenciálně od ní mohly nakazit. V zásadě by organizace měly takto shromážděné osobní údaje návštěvníků použít pouze pro potřeby činnosti hygienických stanic, které plní úkoly podle zákona o ochraně veřejného zdraví. Jakákoliv opatření, která organizace přijme na ochranu před epidemií koronaviru, by měla být přiměřená a šetřit soukromí dotčených osob. Při zpracování osobních údajů platí vždy zásada, že při naplňování jakéhokoli účelu by měly být voleny co nejméně invazivní prostředky, které co nejméně zasahují do soukromí jednotlivců.

## E-shopy, webináře a dobročinné sbírky

Vzhledem k přijatým omezením stále více podnikatelů poskytuje svoje služby on-line nebo zpřístupňuje svoje výrobky k objednání přes e-shop. V případě on-line konference nebo webináře pomocí aplikace nebo jiné platformy, je dobré, aby si účastníci předem ověřili, jak daný poskytovatel zpracovává osobní údaje. A to zejména jaké osobní údaje s ním bude účastník sdílet (např. jména účastníků, zvukový a obrazový záznam), s kým on tyto údaje bude sdílet dál, jestli je organizátor webináře uchovává a na jak dlouho, jaké má zabezpečení osobních údajů apod. Pro organizátory je důležité určit právní důvod pro zpracování osobních údajů účastníků, pokud je nehodlají shromáždit pouze pro účely účasti na webináři a následně je zlikvidovat. Mohlo by jít o zpracování za účelem oprávněného zájmu organizátora webináře, kterým může být i marketing nebo může jít o zpracování, ke kterému je třeba souhlas účastníka, zejména pokud organizátor plánuje dále sdílet osobní údaje účastníků webináře s dalšími obchodními partnery.

S vypuknutím pandemie COVID-19 se napříč Českou republikou vznesla vlna solidarity. Začalo se pomáhat v rámci komunit, i na dálku a to jak sbírkami peněz, tak i zabezpečováním nákupů potravin či zásobováním potřebných dezinfekčními prostředky. V rámci těchto komunitních aktivit se často zejména na sociálních sítích sdílí fotografie a identita obdarovaných nebo pomáhajících. I v takovém případě je třeba respektovat soukromí jednotlivců a zásady GDPR pro zpracování osobních údajů.

**Pokud se Vás některý z výše uvedených problémů dotýká nebo máte jakékoliv jiné otázky spojené se současnou situací, neváhejte se na nás obrátit. Jsme tu pro Vás.**

**Mgr. Karin Pomaizlová**
Partner, Taylor Wessing Praha
Tel: +420 224 81 92 16
k.pomaizlova@taylorwessing.com

**Ing. Mgr. Ivana Taškárová**
Senior Associate, Taylor Wessing Praha
Tel: +420 224 81 92 16
i.taskarova@taylorwessing.com

**Mgr. Martin Loučka**
Senior Associate, Taylor Wessing Praha
Tel: +420 224 81 92 16
m.loucka@taylorwessing.com