Evropská komise

Sedm kroků, které pomohou podnikům

se připravit na obecné nařízení o ochraně osobních údajů

Spravedlnost a spotřebitelé

Komu je tento průvodce určen?

Cílem tohoto průvodce je pomoci firmám, jež údaje nezpracovávají v rámci hlavní činnosti podnikání, tedy například malým a středním podnikům, které nakládají převážně s osobními údaji svých zaměstnanců nebo vedou seznamy klientů a zákazníků. K těmto firmám patří mimo jiné obchodníci či obchody, jako jsou pekařství nebo řeznictví, nebo poskytovatelé služeb, například architekti. V tomto průvodci je vyzdviženo několik kroků, které je třeba učinit v rámci příprav na GDPR.

Osobní údaje jsou informace, které se vztahují ke skutečné žijící fyzické osobě (tedy ne k právnickým osobám). Patří k nim například: jméno, příjmení, adresa bydliště, e-mailová adresa či lokalizační data z mapy na vašem mobilním telefonu. Zpravidla se jedná o údaje, které vedete o svých zaměstnancích, klientech či dodavatelích.

Čím menší riziko představují vaše činnosti pro osobní údaje, tím méně toho musíte udělat

Dodržujte hlavní zásady:

- **Osobní údaje shromažďujte za jasně definovaným účelem a nepoužívejte je k ničemu jinému** (pokud svým klientům řeknete, aby vám poskytli svůj e-mail, na který mohou dostávat vaše nové nabídky či reklamy, nemůžete tento e-mail použít k jinému účelu ani jej prodat jinému podniku).
- **Neshromažďujte více údajů, než je nezbytně nutné** (pokud poskytujete doručovací službu, potřebujete např. adresu, jméno na zvonku, ale už nemusíte vědět, zda dotyčný člověk žije v manželství nebo je svobodný) – zkrátka pamatujte na to, jaké osobní údaje máte pod kontrolou.

KROK 1 — OVĚŘTE SI, JAKÉ OSOBNÍ ÚDAJE SHROMAŽĎUJETE A ZPRACOVÁVÁTE, ZA JAKÝM ÚČELEM A NA JAKÉM PRÁVNÍM ZÁKLADU TO DĚLÁTE

Máte zaměstnance; jejich osobní údaje zpracováváte na základě pracovní smlouvy a na základě zákonné povinnosti (např. ohlašovací povinnost vůči daňovým úřadům / systému sociálního zabezpečení).

Možná vedete seznam **jednotlivých zákazníků**, kterým například zasíláte oznámení o mimořádných nabídkách / reklamních akcích, pokud jste k tomu od nich dostali souhlas.

Ne vždy potřebujete souhlas. Existují případy, kdy fyzické osoby samy očekávají, že jejich údaje budete zpracovávat. Například jako prodejce pizzy možná zpracováváte dodací adresy, na nichž pak inzerujete některé ze svých nových produktů. Tomu se říká oprávněný zájem. Vaší povinností je informovat fyzické osoby o svém zamýšleném použití jejich údajů a přestat takové údaje zpracovávat, pokud vás k tomu vyzvou.

Vedete-li seznam **dodavatelů** nebo **obchodních klientů**, činíte tak na základě smlouvy, kterou jste s nimi uzavřeli. Tyto smlouvy nemusí být nutně v písemné formě.

KROK 2 — INFORMUJTE SVÉ ZÁKAZNÍKY, ZAMĚSTNANCE A DALŠÍ OSOBY O TOM, ŽE JEJICH OSOBNÍ ÚDAJE SHROMAŽĎUJETE

Fyzické osoby musí vědět, že jejich osobní údaje zpracováváte a za jakým účelem to děláte.

Informovat je však nemusíte v případě, že už vědí, jak jejich údaje budete používat. Jedná se například o situaci, kdy vás zákazník požádá, abyste mu něco doručili.

Fyzickým osobám musíte na vyžádání poskytnout rovněž informace o osobních údajích, které o nich vedete, a umožnit jim přístup k nim. Veďte údaje řádně, abyste například svým zaměstnancům mohli snadno a bez problémů poskytnout informace o tom, jaké osobní údaje máte, když vás o to požádají.

KROK 3 — OSOBNÍ ÚDAJE UCHOVÁVEJTE POUZE PO DOBU NEZBYTNĚ NUTNOU

Údaje o vašich zaměstnancích: po dobu zaměstnaneckého vztahu a souvisejících zákonných povinností.

Údaje o vašich zákaznících: po dobu trvání zákaznického vztahu a souvisejících zákonných povinností (například pro daňové účely).

Jakmile pomine účel, pro nějž jste údaje shromažďovali, odstraňte je.

KROK 4 — OSOBNÍ ÚDAJE, KTERÉ ZPRACOVÁVÁTE, ZABEZPEČTE

Ukládáte-li tyto údaje v **systému IT**, omezte přístup k souborům obsahujícím tyto údaje např. heslem. Pravidelně aktualizujte nastavení zabezpečení svého systému.

(Upozornění: GDPR nepředepisuje používání konkrétního systému IT.)

Uchováváte-li fyzické dokumenty s osobními údaji, pak zajistěte, aby k nim neměly přístup nepovolané osoby – zamkněte je v trezoru nebo ve skříni.

KROK 5 — VEĎTE SI DOKUMENTACI O SVÝCH ČINNOSTECH V OBLASTI ZPRACOVÁVÁNÍ ÚDAJŮ

Připravte si krátký dokument s objasněním, jaké osobní údaje máte v držení a z jakých důvodů je vedete. Může se stát, že tuto dokumentaci budete muset předložit vnitrostátnímu úřadu pro ochranu osobních údajů, pokud vás k tomu vyzve.

Tyto dokumenty by měly obsahovat informace uvedené dále.

INFORMACE	PŘÍKLADY
Účel zpracovávání osobních údajů	Upozornění zákazníků na speciální nabídky / zajištění doručení do domu; zaplacení dodavatelům; úhrada platu a sociálního zabezpečení zaměstnancům
Typ osobních údajů	Kontaktní údaje zákazníků; kontaktní údaje dodavatelů; údaje zaměstnanců
Kategorie příslušných subjektů údajů	Zaměstnanci; zákazníci; dodavatelé
Kategorie příjemců	Úřady práce; daňové orgány
Doba uložení	Osobní údaje zaměstnanců do ukončení pracovní smlouvy (a do uplynutí souvisejících zákonných povinností); osobní údaje zákazníků do doby ukončení klientského/smluvního vztahu
Technická a organizační bezpečnostní opatření na ochranu osobních údajů	Pravidelné aktualizace řešení systémů IT; zamčení skříně/trezoru.
Informace, zda jsou osobní údaje předávány příjemcům mimo EU.	Používání procesoru mimo EU (např. pro účely ukládání dat do cloudu)

KROK 6 — UJISTĚTE SE, ŽE PRAVIDLA DODRŽUJÍ I VAŠI SUBDODAVATELÉ

Pokud zadáváte zpracovávání osobních údajů jiné firmě, využívejte pouze takového poskytovatele služeb, který zaručí, že zpracovávání bude probíhat v souladu s požadavky GDPR (např. pravidla zabezpečení). Před uzavřením smlouvy si ověřte, zda tato firma již přešla na GDPR a přizpůsobila se jeho požadavkům. Zaneste to do smlouvy.

KROK 7 — PROZKOUMEJTE, ZDA SE VÁS TÝKAJÍ USTANOVENÍ UVEDENÁ DÁLE

> Organizace si možná budou muset určit pověřence pro ochranu osobních údajů, aby zajistily jejich lepší ochranu. **Pověřence však nemusíte jmenovat**, jestliže zpracování osobních údajů není hlavní součástí vašeho podnikání, nejedná se o rizikové zpracování údajů a vaše činnost není rozsáhlá.

Pokud například ve svém podniku shromažďujete pouze údaje o svých zákaznících, kterým zajišťujete doručení do domu, nemusíte pověřence pro ochranu osobních údajů jmenovat.

Dokonce i když musíte pověřence pro ochranu osobních údajů využít, může jím být stávající zaměstnanec, kterého touto funkcí pověříte vedle jeho dalších úkolů. Nebo jím může být externí poradce, podobně jako řada firem využívá externí účetní.

> **Obvykle nemusíte provádět posouzení vlivu na ochranu osobních údajů**

Toto posouzení vlivu je vyhrazeno pro ty, kdo vystavují osobní údaje většímu riziku, například provádějí velkokapacitní monitorování veřejného prostoru (videodohled).

Jste-li malá firma, která spravuje mzdy zaměstnanců a vede seznam klientů, nemusíte posouzení vlivu na ochranu osobních údajů v případě tohoto zpracování provádět.

Pokuty

Za porušení pravidel ochrany osobních údajů jsou orgány pověřené ochranou osobních údajů oprávněny uvalit sankce. Mohou přijmout nápravná opatření (například vydat nařízení nebo dočasné pozastavení zpracovávání) nebo uložit pokutu.

Jejich rozhodnutí uložit pokutu musí být přiměřené a musí vycházet z posouzení všech okolností daného případu.

Pokud se orgány pověřené ochranou osobních údajů rozhodnou uložit pokutu, musí se její výše také odvíjet od okolností případu, mimo jiné od závažnosti porušení nebo skutečnosti, zda k porušení došlo úmyslně nebo z nedbalosti. V úvahu vezmou také váš postoj a úmysly.

Chcete-li získat více informací:

1. Navštivte online průvodce Evropské komise reformou ochrany osobních údajů – je dostupný ve všech jazycích EU:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_cs

2. Obraťte se na vnitrostátní úřad pro ochranu údajů:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

DŮLEŽITÉ UPOZORNĚNÍ

Informace v tomto průvodci mají přispět k lepšímu pochopení pravidel pro ochranu údajů v EU.

Mají sloužit čistě jako vodítko – právní závaznost má pouze text obecného nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR). Proto pouze GDPR může fyzickým osobám uložit práva a povinnosti. Tyto pokyny nestanoví žádné vymahatelné právo ani očekávání.

Závazná interpretace právních předpisů EU je výlučnou pravomocí Soudního dvora Evropské unie. Názory vyjádřené v těchto pokynech nemají vliv na to, jaké postavení zaujme Komise před Soudním dvorem.

Evropská komise ani žádná osoba, která jedná jejím jménem, nenese odpovědnost za možné použití informací uvedených v tomto průvodci.

Vzhledem k tomu, že tento dokument odráží aktuální stav v době jeho koncipování, je třeba na něj pohlížet jako na „živý nástroj“, který lze vylepšovat a jehož obsah může být bez předchozího oznámení upraven.

Úřad pro publikace

Lucemburk: Úřad pro publikace Evropské unie, 2018

Print	PDF
ISBN 978-92-79-85374-6	ISBN 978-92-79-85395-1
doi:10.2838/230389	doi:10.2838/62652
DS-02-18-544-CS-C	DS-02-18-544-CS-N