Európska komisia

Sedem krokov pre podniky

v rámci prípravy na všeobecné nariadenie o ochrane osobných údajov

Spravodlivosť a spotrebitelia

Pre koho je táto príručka?

Cieľom tejto príručky je pomôcť spoločnostiam, ktoré nespracúvajú osobné údaje v rámci jadra svojej podnikateľskej činnosti, ako sú malé a stredné podniky (MSP), ktoré nakladajú hlavne s osobnými údajmi svojich zamestnancov alebo majú zoznamy klientov a zákazníkov. Týka sa to napríklad obchodníkov či obchodov, ako sú pekáreň alebo mäsiarstvo, respektíve poskytovateľov služieb, ako sú architekti. V tejto príručke nájdete niekoľko krokov, ktoré treba vykonať v záujme prípravy na nariadenie o ochrane osobných údajov (GDPR).

Osobné údaje sú akékoľvek informácie, ktoré sa týkajú reálnej živej osoby (nie právnych subjektov). Zahŕňajú napríklad: meno, priezvisko, adresu bydliska, e-mailovú adresu alebo lokalizačné údaje z mapy na vašom mobile. Toto by typicky mohli byť údaje, ktoré by ste mohli uchovávať o vašich zamestnancoch, klientoch alebo dodávateľoch.

Čím menšie riziko vaše činnosti predstavujú pre osobné údaje, tým menej musíte spraviť

Uplatňujte hlavné zásady:

- **osobné údaje zbierajte na jasne vymedzený účel a nepoužívajte ich na nič iné** (ak si od svojich klientov vypýtate e-mailovú adresu, aby od vás mohli dostávať nové ponuky alebo akcie, túto e-mailovú adresu nesmiete použiť na nič iné ani ju nesmiete predať inému podniku);
- **nezbierajte viac údajov, ako potrebujete** (ak vykonávate doručovanie domov, potrebujete napríklad adresu, meno na zvončeku, ale nepotrebujete vedieť, či je daná osoba v manželskom zväzku alebo slobodná) – jednoducho dbajte na to, aké osobné údaje máte pod kontrolou.

1. KROK — SKONTROLUJTE, AKÉ OSOBNÉ ÚDAJE ZBIERATE A SPRACÚVATE, NA AKÝ ÚČEL TO ROBÍTE, A NA AKOM PRÁVNOM ZÁKLADE

Máte **zamestnancov**. Ich osobné údaje spracúvate na základe pracovnej zmluvy a na základe právnych záväzkov (napr. vykazovanie daňovým orgánom/systému sociálneho zabezpečenia).

Môžete spravovať zoznam **jednotlivých zákazníkov**, napr. na zasielanie oznamov o špeciálnych ponukách/reklamách, pokiaľ ste získali súhlas týchto zákazníkov.

Nie vždy potrebujete súhlas. Sú prípady, keď jednotlivci od vás budú očakávať spracúvanie ich osobných údajov. Napríklad ako predajca pizze môžete spracovať doručovaciu adresu na reklamu niektorého z vašich nových výrobkov. Nazýva sa to oprávnený záujem. Jednotlivcov musíte informovať o vašom plánovanom použití a prestať spracúvať tieto údaje, ak vás o to požiadajú.

Ak spravujete zoznam **dodávateľov** alebo **obchodných klientov**, musíte to vykonávať na základe zmlúv, ktoré s nimi máte. Zmluvy nemajú nevyhnutne písomnú podobu.

2. KROK — INFORMUJTE SVOJICH ZÁKAZNÍKOV, ZAMESTNANCOV A ĎALŠÍCH JEDNOTLIVCOV, KEĎ ZBIERATE ICH OSOBNÉ ÚDAJE

Jednotlivci musia vedieť, že spracúvate ich osobné údaje, a na aký účel ich spracúvate.

Jednotlivcov však netreba nijako informovať, keď už majú informácie o tom, ako použijete údaje, napríklad keď vás zákazník požiada o doručenie domov.

Jednotlivcov tiež musíte na požiadanie informovať o tom, aké osobné údaje o nich uchovávate, a poskytnúť im prístup k ich údajom. Udržujte si poriadok v údajoch, aby ste ich napr. v prípade, že sa váš zamestnanec spýta na to, aký druh osobných údajov máte, vedeli poskytnúť jednoducho a bez nadbytočného úsilia.

3. KROK — OSOBNÉ ÚDAJE UCHOVÁVAJTE LEN TAK DLHO, AKO JE NUTNÉ

Údaje o vašich zamestnancoch: počas trvania pracovnoprávneho vzťahu a súvisiacich právnych záväzkov.

Údaje o vašich zákazníkoch: počas trvania vzťahu so zákazníkom a súvisiacich právnych záväzkov (napr. na daňové účely).

Vymažte údaje, keď viac nie sú potrebné na účely, na ktoré ste ich zozbierali.

4. KROK — ZABEZPEČTE OSOBNÉ ÚDAJE, KTORÉ SPRACÚVATE

Ak uchovávate tieto údaje v **systéme IT**, obmedzte prístup k súborom, ktoré obsahujú tieto údaje, napr. pomocou hesla. Pravidelne aktualizujte bezpečnostné nastavenia vášho systému.

(Poznámka: v GDPR sa nepredpisuje používanie žiadneho konkrétneho systému IT)

Ak uchovávate fyzické dokumenty s osobnými údajmi, uistite sa, že k nim nemajú prístup neoprávnené osoby. Zamknite ich do trezora alebo do skrine.

5. KROK — VEĎTE DOKUMENTÁCIU O VAŠICH ČINNOSTIACH SPRACOVANIA ÚDAJOV

Pripravte krátky dokument, v ktorom spresníte, aké osobné údaje uchovávate a z akých dôvodov. Môže sa od vás vyžadovať, aby ste dokumentáciu sprístupnili vášmu vnútroštátnemu orgánu na ochranu osobných údajov, keď vás o to požiada.

Tieto dokumenty by mali obsahovať informácie uvedené v nasledujúcom texte.

INFORMÁCIE	PRÍKLADY
Účel spracovania osobných údajov	upozornenie zákazníkov na špeciálne ponuky/zabezpečenie doručenia domov; platenie dodávateľom; mzdy a sociálne poistenie pre zamestnancov
Typy osobných údajov	kontaktné údaje zákazníkov; kontaktné údaje dodávateľov; údaje zamestnancov
Kategórie dotknutých osôb	zamestnanci; zákazníci; dodávatelia
Kategórie príjemcov	úrady práce; daňové orgány
Doby uchovávania	osobné údaje zamestnancov do skončenia platnosti pracovnej zmluvy (a súvisiacich právnych záväzkov); osobné údaje zákazníkov do skončenia klientskeho/zmluvného vzťahu
Technické a organizačné opatrenia na ochranu osobných údajov	pravidelná aktualizácia riešení systému IT; zamknutá skriňa/trezor
Či sa osobné údaje prenášajú príjemcom mimo EÚ	využívanie spracovateľa mimo EÚ (napr. na uchovávanie v cloude)

6. KROK — UBEZPEČTE SA, ŽE VÁŠ SUBDODÁVATEĽ DODRŽIAVA PRAVIDLÁ

Ak spracúvanie osobných údajov subdodávateľsky zverujete inej spoločnosti, využívajte iba poskytovateľa služieb, ktorý zaručuje spracúvanie v súlade s požiadavkami GDPR (napr. bezpečnostné opatrenia). Pred podpísaním zmluvy si overte, či už daná spoločnosť zabezpečila zmeny a prispôsobila sa GDPR. Zahrňte to do zmluvy.

7. KROK — SKONTROLUJTE, ČI SA VÁS NETÝKAJÚ UVEDENÉ USTANOVENIA

> Na lepšiu kontrolu osobných údajov môžu byť organizácie povinné vymenovať úradníka pre ochranu osobných údajov (DPO). **Úradníka pre ochranu osobných údajov však nemusíte vymenovať**, ak spracúvanie osobných údajov nie je hlavnou súčasťou vášho podnikania, nejde o rizikové spracúvanie a vaša činnosť nemá veľký rozsah.

Napríklad, ak váš podnik zbiera len údaje o vašich zákazníkoch v rámci doručovania domov, nemusíte vymenovať DPO.

Dokonca aj keď musíte využívať DPO, táto funkcia by sa mohla zveriť existujúcemu zamestnancovi doplnkovo k jeho úlohám. Prípadne to môže byť externý poradca, rovnako ako mnohé organizácie využívajú externých účtovníkov.

> **Za bežných okolností nemusíte vykonávať posúdenie vplyvu na ochranu osobných údajov**

Takéto posúdenie vplyvu je vyhradené pre tých, ktorí predstavujú väčšie riziko pre osobné údaje, napríklad keď vykonávajú rozsiahle monitorovanie verejne prístupnej zóny (napr. bezpečnostný kamerový systém).

Ak ste malý podnik, ktorý spravuje mzdy zamestnancov a zoznam klientov, v súvislosti s týmito operáciami spracovania nemusíte vykonávať posúdenie vplyvu na ochranu osobných údajov.

Pokuty

Orgány dohľadu nad ochranou osobných údajov majú právomoc postihovať porušenie pravidiel ochrany osobných údajov. Môžu prijať nápravné opatrenia (ako je príkaz alebo dočasné pozastavenie spracovania) a/alebo uložiť pokutu.

Ich rozhodnutie uložiť pokutu musí byť pomerné a založené na posúdení všetkých okolností jednotlivého prípadu.

Ak sa rozhodnú uložiť pokutu, výška pokuty bude tiež závisieť od okolností daného prípadu vrátane závažnosti porušenia alebo od toho, či bolo porušenie zámerné alebo spôsobené nedbanlivosťou. Do úvahy sa vezme aj váš postoj a zámery.

Ak si želáte získať ďalšie informácie:

1. navštívte online usmernenia Európskej komisie o reforme ochrany osobných údajov – dostupné vo všetkých jazykoch EÚ:

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

2. obráťte sa na svoj vnútroštátny úrad na ochranu osobných údajov:

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

DÔLEŽITÉ OZNÁMENIE

Informácie a usmernenia v tejto príručke majú prispieť k lepšiemu pochopeniu pravidiel EÚ o ochrane osobných údajov.

Slúžia len na usmernenie – iba znenie všeobecného nariadenia o ochrane osobných údajov (GDPR) má právnu váhu. Znamená to, že iba nariadenie o ochrane osobných údajov môže vytvárať práva a povinnosti jednotlivcov. Tieto usmernenia nevytvárajú žiadne vymožiteľné právo ani očakávanie.

Záväzný výklad právnych predpisov EÚ je vo výlučnej právomoci Súdneho dvora Európskej únie. Názormi vyjadrenými v týchto usmerneniach nie je dotknuté stanovisko, ktoré môže prijať Komisia pred Súdnym dvorom.

Európska komisia ani žiadna osoba konajúca v mene Európskej komisie nenesie zodpovednosť za možné použitie informácií v tejto príručke.

Keďže tento dokument odráža stav vecí v čase jeho zostavovania, mal by sa považovať za „živý nástroj“, ktorý je otvorený pre zlepšenie, a jeho obsah môže podliehať zmene bez oznámenia.

Úrad pre publikácie

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2018

© Európska únia, 2018
Opakované použitie je povolené len s uvedením zdroja.

Print	PDF
ISBN 978-92-79-85387-6	ISBN 978-92-79-85369-2
doi:10.2838/02007	doi:10.2838/65540
DS-02-18-544-SK-C	DS-02-18-544-SK-N