

JE GDPR BYROKRATICKÁ ZÁŤAŽ ALEBO PRAKTICKÁ NEVYHNUTNOSŤ?

Vyžiadala si ho digitálna doba

AUTOR: Henrieta Halasová Bakošová FOTO: archív KK, Dreamstime

OD ÚČINNOSTI EURÓPSKEHO NARIADENIA O GDPR PREŠIEL UŽ ROK, NO MNOHÉ FIRMY EŠTE STÁLE NEVEDIA, ČI SA ICH TOTO NARIADENIE TÝKA ALEBO AKO HO MAJÚ IMPLEMENTOVAŤ. OSLOVILI SME PRETO JUDR. KATARÍNU KROČKOVÚ, KTORÁ SA VENUJE PROBLEMATIKE OCHRANY OSOBNÝCH ÚDAJOV AJ OTÁZKAM OBCHODNÉHO REGISTRA ČI PRACOVNÉHO PRÁVA.





Dodnes veľa firiem nemá jasno v tom, čo všetko sú osobné údaje a koho sa nariadenie týka. Tak si to pre istotu na úvod zopakujme.

Áno, prešiel už rok, no stále sa stretávame s otázkou, čo je GDPR, čo osobné údaje a či je naozaj potrebné mať „vypracovanú dokumentáciu“. Klienti majú často problém s tým, že zdanlivo ide o ďalšiu byrokratickú záťaž zo strany štátu. Dá sa povedať, že GDPR sa týka každej spoločnosti, niektorej viac, niektorej menej. Všetko závisí od toho, aké údaje spracúva aj od odvetia činnosti konkrétneho klienta. Iné osobné údaje spracúva lekár a iné výrobná spoločnosť.

Je potrebné, aby sa firmy postavili k tejto problematike zodpovedne. Často spracúvajú osobné údaje, ktoré nepotrebujú, databázy nie sú aktualizované, nemajú právne základy na spracúvanie a o bezpečnosti nemôže byť v mnohých prípadoch ani reč. Firmy nemajú nastavené žiadne procesy, všetci robia všetko a podobne.

Ochrana osobných údajov však patrí k základným ľudským právam. Každý z nás by mal chrániť seba a svoje údaje, tak isto by aj spoločnosti mali chrániť svoje know-how. Ochranu týchto práv nám zaručuje Občiansky zákonník, ako aj Ústava Slovenskej republiky. Ochrana osobných údajov sme tu mali aj pred účinnosťou nariadenia. Dovolím si povedať, že už zákon 122/2013 Z. z. bol dosť prísny, avšak Nariadenie EÚ o GDPR z roku 2016 a účinné od 25. mája 2018 poníma ochranu osobných údajov komplexnejšie. Ochrana osobných údajov je potrebná, žijeme v digitálnej dobe



a dobe sociálnych sietí a ak potrebujeme niečo nájsť, jednoducho si to nájdeme online. Ďalším problémom pri slabej ochrane osobných údajov môže byť rôzna trestná činnosť súvisiaca s ukradnutou identitou využívanou napríklad pri nelegálnej migrácii, obchodovaním s ľuďmi a inou protizákonnou činnosťou.

Osobné údaje sú definované v Článku 4 odsek 1 Nariadenia GDPR, a to nasledovne: Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“). Identifikovateľnou fyzickou osobou sa rozumie osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné

údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Doplnila by som, že podľa Nariadenia sú osobnými údajmi aj e-mailová adresa a cookies.

Mnohí si nedokážu predstaviť, čo presne znamená implementácia nariadenia. Ako prebieha tento proces?

K tejto otázke by som rada podotkla, že GDPR je živé odvetvie a jeho implementácia určite nepredstavuje hárok papiera, ktorý si založíte do zásuvky pre prípad kontroly, ako si mnohí myslia. Treba nastaviť procesy v spoločnosti. Úrad na ochranu

osobných údajov priebežne vydáva metodické pokyny k rôznym problematikám, napríklad k zákonnosti spracúvania údajov, k povinnostiam prevádzkovateľa e-shopu či k spracúvaniu osobných údajov školami, taktiež vyjadrenia k fotografiám.

Implementácia GDPR by mala vychádzať z pozície vedenia spoločnosti. Ochrana osobných údajov v praxi vyplýva z legislatívnych podmienok a z podmienok činnosti spoločností (prevádzkovateľov). Implementovať GDPR znamená, že prevádzkovateľ – spoločnosť (firma), pozná toky dát obsahujúce osobné údaje (analýza), informuje dotknuté osoby o spracúvaní osobných údajov, poučí oprávnené osoby, má uzatvorené sprostredkovateľské zmluvy s dodávateľmi o spracovaní osobných údajov, realizuje technické, organizačné a bezpečnostné opatrenia zabezpečujúce ochranu osobných údajov pri všetkých formách ich spracúvania, či už ide o digitálnu alebo papierovú. Taktiež má firma DPO, teda zodpovednú osobu, ak to je zákonom ustanovené.

Dokážu si firmy poradiť s implementáciou aj samy alebo nevyhnutne potrebujú odbornú pomoc?

Spoločnosti majú dve možnosti. Buď vyriešia problematiku GDPR prostredníctvom externej spoločnosti, ktorá im vypracuje dokumentáciu presne podľa požiadaviek a činnosti spoločnosti alebo prostredníctvom vlastných zdrojov prostredníctvom zamestnanca. Upozorňujem však, že by mal mať znalosti z predmetnej legislatívy a skúsenosti z oblasti bezpečnosti.

V prípade našej kancelárie sme v pozícii externého subjektu. Najskôr urobíme komplexný audit, určí sa tok osobných údajov, kde sa zistí aktuálny stav súvisiaci so spracúvaním osobných údajov spoločnosťou. Tento audit sa vykonáva priamo u klienta,

” **Ochrana osobných údajov patrí k základným ľudským právam. Každý z nás by mal chrániť seba a svoje údaje, tak isto by aj spoločnosti mali chrániť svoje know-how.**





” Najvyššia pokuta, ktorú môže Úrad na ochranu osobných údajov uložiť, je do dvadsať miliónov eur.

keď nám klient odpovedá na otázky, ktoré nás nasmerujú ku konkrétnym nástrojom. Na ich základe implementujeme Nariadenie GDPR pre danú spoločnosť.

Implementácia konkrétne obsahuje identifikáciu spracúvaných osobných údajov, analýzu bezpečnosti informačných systémov u prevádzkovateľa a aj posúdenie vplyvov na ochranu údajov (tzv. Data Protection Impact Assessment, skrátene DPIA), ktoré sa vyžaduje pri špecifickom, tzv. systematickom spracúvaní osobných údajov: pri automatizovanom spracúvaní dát, spracúvaní osobných údajov vo veľkom množstve a pri systematickom monitorovaní verejne prístupných miest vo veľkom rozsahu. Týka sa to činností, ako napríklad spracúvanie biometrických údajov fyzických osôb, spracúvanie genetických údajov fyzických osôb, systematické kamerové monitorovanie verejných priestorov (v jednotlivých mestách, obciach a dopravcami mestskej a prímestskej verejnej dopravy), sledovanie osôb súkromnými detektívnymi, resp. bezpečnostnými službami.

Ďalej sa nastavuje ochrana osobných údajov v súvislosti s informačnými systémami a vypracovanie návrhov bezpečnostných opatrení, ako napríklad: personálne a organizačné opatrenia, likvidácia osobných údajov, zálohovanie a, samozrejme, kontrolný mechanizmus.

Čo by mali v súvislosti s nariadením vedieť obchodníci? Čo je pre nich obzvlášť dôležité?

Ako som spomenula v otázke č. 1, Nariadenie GDPR sa týka skoro každého podnikateľského subjektu, ktorý spracúva osobné údaje, pričom dodržiavané by malo byť Nariadenie a aj Zákon. Spomenula by som pár príkladov vo všeobecnosti – poučenie zamestnancov, splnenie informačnej povinnosti voči dotknutej osobe, spracúvanie osobných údajov na základe zásad, určenie účelov spracúvania a ich právne základy, aby vykonal personálne, organizačné a technické opatrenia.

Vzhľadom na to, že každý prevádzkovateľ má určité špecifiká, je potrebné, aby boli zapracované do dokumentácie GDPR. Tak, ako všetky spoločnosti, aj obchodná spoločnosť má svoje špecifiká. V každom prípade však tieto spoločnosti nakladajú s osobnými údajmi, napríklad v prípade zamestnancov, klientov alebo kamerových systémov.

V neposlednom rade je potrebné vykonať aj školenie zamestnancov spoločnosti v súvislosti so zásadami a princípmi v oblasti GDPR na základe metodiky – smernice v uvedenej problematike vypracovanou spoločnosťou.

Treba sa báť v súvislosti s GDPR nejakej kontroly? Je nezavedenie nariadenia postihnuteľné?

Povinnosť implementácie je od 25. 5. 2018. Ak tak niektorá spoločnosť neurobila, treba si v prvom rade uvedomiť, že môže dôjsť k úniku osobných údajov a ich následnému zneužitiu. Čo sa týka kontroly, najvyššia možná pokuta, ktorú môže Úrad na ochranu osobných údajov uložiť, je do dvadsať miliónov eur, alebo ak ide o podnik, tak do štyroch percent celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia. ✕

Kto je Katarína Kročková

✓ Vyštudovala právo na Právnickej fakulte Univerzity Komenského v Bratislave. Počas štúdií pracovala ako personalistka, neskôr zastávala post korporátneho právnika. Problematike ochrany osobných údajov sa venuje niekoľko rokov a poskytuje konzultácie a komplexné riešenia pri implementácii GDPR. Okrem tejto témy sa venuje pracovnému právu, otázkam obchodného registra a mediácii. V roku 2016 založila spoločnosť Kročka & Partners, v ktorej spolupracuje s expertmi na pracovné právo a bezpečnosť ochrany osobných údajov v online prostredí. Je spoluautorkou publikácie Judikatúra v pracovnoprávných veciach (2018), ktorá slúži personalistom, advokátom, zamestnávateľom a zamestnancom ako pomôcka v otázkach ukončenia pracovného pomeru. V súčasnosti sa spoluautorsky podieľa na publikácii Judikatúra v oblasti konania obchodných spoločností (predpokladaný termín: jeseň/zima 2019).