Usmernenie CED týkajúce sa implementácie všeobecného nariadenia o ochrane údajov

Zameranie na osoby zodpovedné za ochranu údajov

Február 2018

Súvislosti

- Všeobecné nariadenie o ochrane údajov (GDPR) (Nariadenie (EÚ) 2016/679) je nariadením, ktorým Európsky parlament, Rada Európskej únie a Európska komisia majú v úmysle posilniť a zjednotiť ochranu údajov pre všetky subjekty v rámci EÚ.
- Nariadenie - v kapitole IV, oddiel 4, články 37-39 - špecifikuje požiadavky o určení, postavení a úlohách osôb zodpovedných za ochranu údajov (DPO).

Prečo je to dôležité pre zubných lekárov?

- Príslušné vnútroštátne orgány majú za povinnosť implementovať ustanovenia GDPR a mohli by vyžadovať, aby zubné ambulancie stanovili osobu zodpovednú za ochranu údajov.
- Zatiaľ čo podľa usmernenia pracovnej skupiny pre ochranu údajov poradný orgán pre spracovanie osobných údajov (zriadený smernicou č. 95/46/EHS) - uvádza, že jednotliví lekári (to isté by sa vzťahovalo aj na zubných lekárov) nepotrebujú osobu zodpovednú za ochranu údajov, členské štáty nie sú viazané týmto usmernením, pričom nie je jasné, kedy je potrebné vymenovať DPO.
- V závislosti od národnej implementácie by to mohlo viesť k zvýšeniu administratívy a finančného zaťaženia jednotlivých zubných lekárov.

Časová os

- Nariadenie bolo uverejnené v apríli 2016.
- Účinnosť je od 25. mája 2018.

Požadovaná akcia

- Spojte sa so úradom na ochranu údajov a zistite, v akom stave implementácie sú a ich názor na DPO.
- Identifikujte funkčné riešenie pre zubných lekárov (t. j. definujte prah pre požadovanie DPO pomocou nižšie uvedeného návodu) vo vašich národných kontextoch a poskytnite ho orgánom.

Odporúčania

- Vo všeobecnosti CED zdôrazňuje, že k ochrane údajov treba pristupovať s vážnosťou. Údaje o pacientoch musia byť maximálne chránené.

Zodpovedná osoba pre ochranu údajov

- V GDPR sa uvádza, že osoba zodpovedná za ochranu údajov by mala byť vymenovaná vtedy, ak základné činnosti prevádzkovateľa alebo sprostredkovateľa (v našom prípade zubná ambulancia (zdravotnícke zariadenie) alebo zubného lekára) pozostávajú zo spracovania dát, ktoré vo veľkej miere vyžadujú pravidelné a systematické monitorovanie dát dotknutých osôb.
- Preto v procese posudzovania, či DPO je potrebný, treba vziať do úvahy dve kritériá:

- Koľko ľudí v rámci zubného lekárstva má vo svojom popise základných činností spracovanie údajov?
- Spracováva sa veľké množstvo údajov?

o **Kritérium 1: Hlavná činnosť**

- Podľa nášho názoru základnou činnosťou zubného lekára je poskytovanie zubnej starostlivosti pacientom (skutočná základná činnosť) a nie spracovávanie údajov. Zároveň zubní lekári môžu mať zamestnancov, ktorých základnou činnosťou je spracovanie dát pacientov. Ak zubný lekár nemá viacerých zamestnancov, ktorých popisom práce by bolo spracovanie údajov, osoba zodpovedná za ochranu údajov by sa nemala vyžadovať.

o Kritérium 2: Množstvo spracovávaných dát

- Pracovná skupina uvádza ďalšie usmernenia, ako definovať množstvo spracovávaných dát:
- Počet dotknutých osôb - buď ako konkrétny počet alebo v pomere k príslušnej populácii
- Objem údajov a / alebo rozsah spracovávaných dátových položiek
- Doba trvania alebo stálosť spracovania údajov
- Geografická rozloha spracovania údajov
- Minimálne dve z týchto kritérií by mali dokázať, že dotknutý subjekt spracováva mimoriadne množstvo údajov, a preto sa bude vyžadovať ustanovenie funkcie DPO. Priemerná zubná ambulancia by sa preto nemala považovať za miesto, kde sa spracovávajú údaje vo veľkom rozsahu.

Posúdenie vplyvu ochrany údajov

Sme presvedčení, že na posúdenie, či požadované požiadavky sú splnené, by sa mali uplatňovať rovnaké kritériá zavedené GDPR pre tzv. posúdenie vplyvu ochrany údajov (DPIA) - kapitola IV, oddiel 3, články 35 - 36 – ak by použitie nových technológií na spracovanie údajov pravdepodobne ohrozilo práva a slobodu osôb.

Ak potrebujete podporu od kancelárie CED, neváhajte nás kontaktovať.

****

Súvislosti - hlavné zmeny v GPDR a v čom líšia od predchádzajúcej smernice

(Zdroj: https://www.eugdpr.org/the-regulation.html)

Sankcie

Nariadenie stanovuje dve horné hranice pre pokuty za nedodržiavanie pravidiel: 1) pokuty do 10 miliónov EUR, alebo v prípade podniku do 2% celoročného obratu. Prvá kategória pokuty by sa mala uplatňovať napríklad v prípade prevádzkovateľa, ak nevykonávajú posúdenie

vplyvu tak, ako to vyžaduje nariadenie; 2) maximálne 20 miliónov EUR alebo 4% celoročného obratu. Príkladom by mohlo byť porušenie práv dotknutých osôb podľa nariadenia. Pokuty sú nastavené podľa okolností každého jednotlivého prípadu.

Právo na prístup

Súčasťou rozšírených práv dotknutých osôb uvedených v GDPR je právo požadovať od prevádzkovateľa potvrdenie či sú ich osobné údaje spracovávajú alebo nie, kde a za akým účelom. Okrem toho prevádzkovateľ poskytne bezplatne elektronickú kópiu osobných údajov. Táto zmena je dramatickým posunom k transparentnosti údajov a posilnenie postavenia osôb poskytujúcich svoje osobné údaje.

Právo na zabudnutie

Právo na zabudnutie, známe aj pod názvom výmaz údajov, oprávňuje dotknutú osobu na to, aby prevádzkovateľ vymazal osobné údaje tejto osoby, zastavil ďalšie šírenie týchto údajov a tiež zabezpečil, aby potenciálne tretie strany taktiež pozastavili spracovanie týchto údajov. Podmienky pre výmaz, ako je uvedené v článku 17, zahŕňajú údaje, ktoré už nie sú relevantné pre pôvodné účely spracovania alebo to, že oprávnené osoby stiahli svoj súhlas na spracovanie ich údajov. Treba vziať na vedomie, že toto právo si vyžaduje, aby pri posudzovaní takýchto žiadostí prevádzkovatelia porovnali práva osôb s verejným záujmom na dostupnosti údajov.

Ochrana osobných údajov špecificky navrhnutá

Ochrana osobných údajov ako koncept existuje už niekoľko rokov, ale len teraz sa stáva súčasťou zákonovej požiadavky v rámci GDPR. Vo svojej podstate si ochrana súkromia v štádiu návrhu vyžaduje začlenenie ochrany údajov od začiatku navrhovania systémov, nie len ako dodatok. Konkrétnejšie – „Prevádzkovateľ musí ... uplatniť vhodné a účinné technické a organizačné opatrenia ... v záujme splnenia požiadaviek tohto nariadenia a ochrany práv dotknutých osôb“. Článok 23 vyžaduje, aby prevádzkovatelia uchovávali a spracovávali iba údaje, ktoré sú absolútne nevyhnutné na splnenie ich povinností (minimalizácia údajov), ako aj obmedzovali prístup k osobným údajom osobám, ktoré ich spracovávajú.

Osoby zodpovedné za ochranu údajov

V súčasnosti sú prevádzkovatelia povinní oznámiť svoje činnosti spojené so spracovaním údajov miestnym DPA (u nás úrad na ochranu osobných údajov), čo môže byť pre nadnárodné spoločnosti byrokratickou nočnou morou, keďže väčšina členských štátov EÚ má rozdielne požiadavky týkajúce sa tohto oznamovania. V súlade s GDPR nebude potrebné podávať oznámenia / alebo registrácie u jednotlivých miestnych DPA v súvislosti s činnosťami spojenými so spracovaním údajov, ani sa nebude vyžadovať oznamovanie / získanie súhlasu na transfery na základe vzorových zmluvných ustanovení (MCC). Namiesto toho budú existovať interné požiadavky na vedenie záznamov, ako je ďalej vysvetlené nižšie, a vymenovanie DPO bude povinné len pre tých, prevádzkovateľov a sprostredkovateľov, ktorých hlavné činnosti spočívajú v spracovávaní údajov, ktoré si vyžadujú pravidelné a systematické monitorovanie

osobných údajov vo veľkom množstve alebo osobitné kategórie údajov, alebo údajov týkajúcich sa trestných sankcií a trestných činov.

DPO:

o Musia byť vymenovaní na základe odborných kvalít a najmä znalosti právnych predpisov a postupov v oblasti ochrany údajov

o Môže byť zamestnancom alebo externým poskytovateľom služieb

o Kontaktné údaje musia byť poskytnuté príslušnému orgánu pre ochranu údajov

o Musia mať k dispozícii primerané zdroje na plnenie svojich úloh a udržiavanie ich odborných znalostí

o Musia sa hlásiť priamo na najvyššiu úroveň riadenia

o Nesmie vykonávať žiadne iné úlohy, ktoré by mohli viesť ku konfliktu záujmov.

Oznamovanie narušenia bezpečnosti

V rámci GDPR bude oznámenie o narušení bezpečnosti povinné vo všetkých členských štátoch tam, kde je pravdepodobné, že narušenie bezpečnosti môže „viesť k ohrozeniu práv a slobôd jedincov“. Oznámenie sa musí podať do 72 hodín od momentu zistenia narušenia bezpečnosti. Sprostredkovatelia budú tiež povinní neodkladne informovať svojich zákazníkov hneď po tom, ako zistia narušenie bezpečnosti údajov.

Prenosnosť údajov

GDPR zavádza prenosnosť údajov - právo dotknutej osoby prijímať osobné údaje, ktoré sa ich týkajú, ktoré predtým poskytli v bežne používanom a strojovo čitateľnom formáte a majú právo poslať tieto údaje inému prevádzkovateľovi.