



RODO w sektorze medycznym

Marzec 2, 2017

Dzisiaj byłam na szkoleniu organizowanym przez GIODO dla administratorów bezpieczeństwa informacji z sektora medycznego. Jeśli działasz w tej branży (opieka zdrowotna, stomatologiczna, placówki medyczne, firmy dostarczające soft czy IT dla branży medycznej) to mam dla Ciebie kilka ważnych informacji.

IOD w pierwszej linii

O tym kiedy należy wyznaczyć ABI a kiedy jest to fakultatywne możesz dowiedzieć się łatwo z przepisów jak i oczywiście z Pomocnika RODO (kliknij [tutaj](#)). Natomiast to co jest istotne w świetle nowych przepisów to, że za faktyczną rozliczalność Administratora Danych będą odpowiadali Inspektorzy Ochrony Danych (obecni ABI). To inspektor **będzie stał na pierwszej linii frontu** i z podmiotem danych i organem kontrolnym i co więcej praktycznie każdy proces przetwarzania będzie musiał oceniać pod kątem zgodności przetwarzania danych. Warto zatem zdać sobie sprawę, że Inspektor będzie miał dużo więcej pracy niż obecny ABI co wiąże się nie tylko ze wzrostem obowiązków, ale i odpowiedzialności.

Dane szczególnej kategorii

RODO określa czym są dane genetyczne, dane biometryczne, dane dotyczące zdrowia ([tutaj](#) szczegółowe wyjaśnienie). Dzisiaj wielu ABI reagowało z zaskoczeniem, że dane

dotyczące zdrowia to już np. sama informacja o tym, że osoba leczy się u danego lekarza. Tak. **To jest dana szczególnie chroniona** w myśl RODO. W przepisach jest jasno bowiem napisane, że dane szczególnej kategorii to także informacje o zarejestrowaniu danej osoby fizycznej celem świadczenia usług opieki zdrowotnej.

Co to oznacza w praktyce?

Już sam fakt, że ktoś jest zapisany do stomatologa czy lekarza stanowi daną szczególnie chronioną. Stąd poziom ryzyka przetwarzania tych danych jest większy. Ma to ogromne znaczenie np. przy wyborze systemu IT do rejestracji pacjentów czy wybrania firmy, która oferuje usługę chmurową rejestracji pacjentów. Firma informatyczna jako procesor będzie musiała wykazać, że ma odpowiednie standardy ochrony danych wdrożone. Jeśli tego nie będzie miała, **organ kontrolny będzie mógł kwestionować** jej wybór i nałożyć jak wiemy różne środki przymusu, na karze finansowej kończąc.

Kiedy można przetwarzać takie dane?

- Nowością, o czym pisałam już wielokrotnie jest **zgoda wyrażona w dowolnej formie**. Warunek zgody jaki musi być spełniony to musi być to zgoda wyraźna i oczywiście nie obarczona wadą oświadczenia woli. Pamiętajmy zatem by prawidłowo zbudować klauzule zgody by komunikat był jasny dla przeciętnego konsumenta o zakresie, celu i zasadzie przetwarzania danych.
- Przepis prawa
- Ważny interes publiczny
- Ochrona żywotnych interesów osoby (szczególnie istotne gdy podmiot danych nie może wyrazić zgody ze względu na swój stan psychofizyczny a zachodzi potrzeba przetwarzania danych na potrzeby np. ratowania życia)
- Ochrona zdrowia rozumiana szerzej czyli nie tylko procedury medyczne, ale także polityka zdrowotna – np. zabezpieczenie populacji przed chorobami, ochrona zdrowia, taryfikacja świadczeń zdrowotnych
- Badania naukowe, ale dalej idące wymagania w zakresie ochrony danych są w przypadku takiego przetwarzania niż te które są obecnie
- Dane statyczne
- Dane podane do wiadomości publicznej tylko o podmiotach danych jeżeli oczywiście świadomie i celowo podmiot danych podał do wiadomości publicznej ten dane (np. ktoś sam napisał na profilu społecznościowym, że jest chory na jakąś chorobę)
- Dochodzenie praw przed sądem, realizacja orzeczenia sądowego czy podjęcie obrony przed roszczeniami (w zakresie gromadzenia materiału na potrzeby rozstrzygania ewentualnych roszczeń)
- Umowa z pracownikiem służby zdrowia (np. w zakresie profilaktyki zdrowotnej, diagnozy medycznej itp.)

Powierzenie

Warto pamiętać, że nie tylko personel medyczny jest zobowiązany do zachowania tajemnicy, ale także podpisując umowę z IT trzeba nałożyć obowiązek zachowania poufności.

Na poziomie RODO możliwe będzie także zlecenie na zewnątrz usług elektronicznego przetwarzania (powierzenie) przez upoważniony podmiot prowadzący rejestr medyczny co

obecnie na gruncie art. 20 ust. 8 ustawy o systemie informacji w ochronie zdrowia nie jest możliwe ([tekst ustawy](#))

Podmioty wyspecjalizowane w zapewnianiu obsługi technicznej systemów teleinformatycznych, o których mowa w ust. 5 (czyli upoważniony podmiot prowadzący rejestr medyczny), nie mogą powierzać innym podmiotom przetwarzania danych zawartych w rejestrach medycznych.

Warto oczywiście pamiętać, że podpowierzenie będzie musiało odbywać się **wyłącznie za zgodą** czyli na poziomie umowy z podmiotem prowadzącym rejestr medyczny Administrator Danych będzie wyrażał zgodę albo odpowiednio aneksował umowę.

Oczywiście pamiętajmy, że krajowe przepisy mogą się zmienić jeśli ustawodawca będzie chciał je dostosować do przepisów rozporządzenia. Jeśli to nie nastąpi to i tak pierwszeństwo mają przepisy rozporządzenia.

Więcej obowiązków

Tak jak pisałam Inspektor Ochrony Danych (obecny ABI) będzie miał więcej obowiązków. Administrator, który nie wyznaczy IOD będzie oczywiście musiał sam się uporać z tymi obowiązkami.

Natomiast to co jest ważne to trzeba sobie już teraz ułożyć proces by spokojnie realizować zadania jakie nakłada RODO.

Podmiot danych będzie miał teraz 30 dni na otrzymanie odpowiedzi o tym jakie dokładnie dane na jego temat są przetwarzane. Obowiązuje tu zasada przejrzystej komunikacji, prostego i jasnego języka. Jeśli odpowiedź będzie bardziej skomplikowana można wydłużyć odpowiedź do 2 miesięcy, ale organ kontrolny będzie to skrupulatnie badał (tak dzisiaj na szkoleniu zostało zapowiedziane ;).

Dopiero jeśli ktoś zbyt często będzie wносił zapytania albo będą one ewidentnie nieuzasadnione (pyta o to samo choć dostał już raz odpowiedź) to będzie można wprowadzić opłatę za udzielenie odpowiedzi. I to taką, która stanowi równowartość kosztów. W ostateczności ADO będzie mógł odmówić udzielenia informacji.

Na stronach internetowych jak i w widocznych miejscach stacjonarnie trzeba będzie podać dane kontaktowe IOD co wielu przyszłym inspektorom niezbyt się podoba. Pewnie będą atakowani super szkoleniami i ofertami. No i oczywiście zapytaniami od podmiotów danych. Dlatego dobrą praktyką jest by e-mail był ogólny, np: iod@nazwafirmy.pl i by już teraz przygotować się na to, że na taką pocztę będzie przychodziło trochę spamu.

Czas przetwarzania

To o czym ja już piszę w klauzulach zgody, a co wymaga RODO to określenie czasu przetwarzania danych. W przypadku sektora medycznego można zrobić odesłanie do

przepisów regulujących, ale także można wskazać przesłanki kiedy dane nie będą przetwarzane.

Prawo do przenoszalności

Istotną kwestią jest też to, że jeżeli następuje np. kontynuacja leczenia to oczywiście dane są przenoszone do innego Administratora. Na gruncie obecnych przepisów mówimy w takiej sytuacji o udostępnieniu. Ewentualnie przekazujemy pacjentowi historię choroby, a on sam może iść z dokumentacją do innego lekarza.

RODO zakłada, że jeżeli podmiot danych zażąda by jego dane będą zostały przeniesione to ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe go dotyczące, których dostarczył administratorowi, oraz ma prawo przesłać te dane innemu administratorowi. W praktyce oznacza to **nieco więcej pracy niż teraz**. Jednak co ważne będziemy mogli utrzymać status quo i zastosować wyłączenie zasłaniając się tajemnicą zawodową i tym samym wywiązanie się z obowiązku prawnego, które wyłącza prawo do przenoszalności danych.

Profilowanie

Profilowanie danych szczególnych kategorii jest zabronione chyba, że jest wyraźnie udzielona zgoda przez podmiot danych czy odbywa się to ze względu na ważny interes publiczny (pojęcie szerokie). Organy nadzorcze będą dążyły do maksymalnego ściśnięcia, zawężenia tego pojęcia interesu publicznego.

Prawo do bycia zapomnianym

Wyłączone jest przy przetwarzaniu danych dla celów medycznych, w tym chodzi tutaj o względy interesu publicznego w dziedzinie zdrowia publicznego.

Monitoring wizyjny w placówkach medycznych

Trzeba będzie określić w drodze odpowiedniej polityki zasady prowadzenia monitoringu, jak są przechowywane dane, kto ma do nich dostęp, kiedy są usuwane i w jaki sposób etc. Z pomocą może przyjść także ustawa o monitoringu wizyjnym. Jednak to takie trochę Yeti póki co. Wszyscy mówią, że będzie ale jak jej nie ma tak nie ma ;).

Zabezpieczanie dokumentacji przekazywanej drogą elektroniczną

Organ nadzorczy jasno wskazał na co będzie zwracał uwagę. Szybko wypunktuję:

1. Czy jest prawidłowa autoryzacja (podpis elektroniczny / profil zaufany – identyfikacja)
2. Czy podmiot, który powinien odebrać faktycznie odebrał (potwierdzenie dla celów dowodowych)
3. Czy jest zachowana poufność transmisji (dane w transporcie czy są szyfrowane)

Kontrole

Jak będą wyglądały? To chyba interesuje każdego i to niezależnie od sektora. Aktualnie przebieg kontroli wygląda tak:

- Żądanie złożenia wyjaśnień / przesłuchuje się kierowników, pracowników itp.
- Wgląd do dokumentów / umowy, procedury, wewnętrzne regulacje
- Przeprowadzenie oględzin / system informatyczny i sprawdzenie jakie dane są przetwarzane i czy są właściwie zabezpieczone, oględziny archiwów, serwerowni itd.
- Wstęp do pomieszczeń
- Zlecenie sporządzenia ekspertyz i opinii / rzadko się zdarza

Sama kontrola to oczywiście co najmniej 1 prawnik + 1 informatyk i oczywiście musi być odpowiednia legitymacja + upoważnienie do przeprowadzenia kontroli (np. jest wskazane, że kontroli będzie podlegać rodzaj przetwarzanych danych albo sposób itp.). Organ uprzedza o kontroli (7 dni przed).

Jak to będzie wyglądało w świetle RODO? Zobaczymy. Czekamy na projekt ustawy, który ma regulować zasady działania organu kontrolnego.

Kilka przykładów z inspekcji

Korzystając z okazji napiszę tutaj o trzech przypadkach, które niedawno podlegały kontroli GIODO.

Login i hasło w tajemnicy

Kontrola wykazała, że w kadrach dwie osoby dzieliły ze sobą biuro. Każda miała swój komputer i odrębny login i hasło. Jedna zajmowała się listą płac a druga wydrukami do ZUS. Jednak obie Panie miały podłączenia do różnych drukarek i by nie robić problemów przekazały sobie wzajemnie loginy i hasła do swoich komputerów. Organ oczywiście stwierdził, że to uchybienie.

Wyciek danych a procedury

Lekarz wystawiający zwolnienia lekarskie dysponował bloczkiem z zapisanymi zwolnieniami, które zgubił. Ktoś jednak je odnalazł i wniósł skargę. Okazało się, że lekarz pracował w szpitalu i prywatnej placówce. Szpital stwierdził, że ADO w tym wypadku jest lekarz i nie ma problemu. Oczywiście GIODO nakazał szpitalowi wprowadzenie procedur bo to szpital jest ADO. Prywatna placówka medyczna wprowadziła procedurę by korzystać z wewnętrznego bloczka placówki i deponować go w odpowiednim miejscu.

Kto i co może?

GIODO interweniował na polecenie Rzecznika Praw Pacjenta w placówce gdzie rejestracja miała dostęp do karty historii choroby pacjenta. Oczywiście organ kontrolny uznał, że ten personel miał prawo przetwarzać takie dane co wynika z przepisów.

Migracja danych

Szpital wynajmował pomieszczenia opieki zdrowotnej i zakład ten się przeniósł do nowej lokalizacji zostawił niespodziankę w postaci całej dokumentacji i nie zamierzał tego odebrać. Po skardze szpitala GODO nakazał zabezpieczenie dokumentacji + zgłosił sprawę do prokuratury. Dopiero to spowodowało, że zakład zainteresował się danymi pacjentów.

RODO tuż tuż

—

Autor grafiki promującej wpis: [Richard de Ruijter](#)