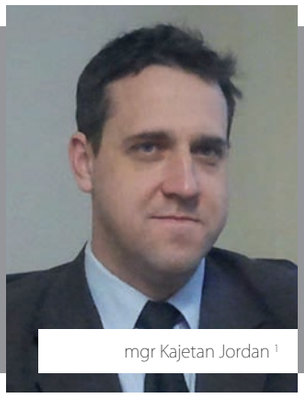

mgr Kajetan Jordan [1]

System ochrony danych osobowych w sektorze medycznym.

The protection system of personal data in the medical.

[1] Information Security Manager, Certyfied ISO 27001 Lead Auditor, IT PM
STANDARDER Sp. z o.o.
ul. Kolista 25 40-486 Katowice
e-mail: info@standarder.pl
tel. 32 320 29 07

Słowa kluczowe:
dane osobowe, system, prywatność przy projektowaniu, prywatność wartością domyślną, dokumentacja medyczna, cykl deminga

Key words:
Personal data., system, privacy by design, privacy by default, medical records, Deming cycle

Kilka lat temu w gronie przyjaciół zastanawialiśmy się skąd bierze się „rozluźnienie obyczajów" w ochronie danych osobowych w sektorze medycznym . Rozważaliśmy przypadki zarówno w placówkach publicznych jak i prywatnych. O ile w przypadku placówek publicznych padały argumenty wskazujące na potencjalne przelewanie pieniędzy publicznych pomiędzy własnymi sakwami, o tyle w placówkach prywatnych trudno było o jakąkolwiek argumentację. Dla mnie, osoby zajmującej się bezpieczeństwem informacji sytuacja wydaje się być szczególnie interesująca ze względu na przetwarzanie danych ze szczególnej kategorii tzw. „wrażliwych", dotyczących stanu zdrowia.

Jednym z powodów wydaje się brak konieczności rejestrowania zbiorów danych osobowych w ogólnokrajowym, jawnym rejestrze zbiorów danych osobowych GIODO? Błędnie rozumiane zwolnienie może powodować poczucie braku konieczności ochrony tychże danych. Na podstawie Art. 43 ust. 1 pkt. 5 z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych zawierające informacje dotyczące osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta. Zaznaczyć przy tym należy dwie kwestie. Po pierwsze odnosi się to wyłącznie do zbioru danych przetwarzanego w tymże celu. Dla placówek prywatnych rozważyć należy przetwarzanie innych zbiorów danych osobowych, np. dla celów marketingowych. W tym przypadku nie ma już podstawy prawnej do zwolnienia z obowiązku rejestracji. Po drugie, brak obowiązku rejestracyjnego nie zwalnia Administratora Danych z obowiązku ochrony danych osobowych w zbiorze. Mało tego, ze względu na kategorię przetwarzanych danych podlegają one ochronie na wyższym poziomie.

Drugim z powodów są „nawyki" branżowe. Argumentacja „tak było do tej pory" niestety nie zwalnia Administratora Danych z obowiązku ochrony. Wydaje się nawet że wręcz przeciwnie, świadczy o braku świadomości w zakresie ochrony danych osobowych.

Streszczenie

W jaki sposób zbudować skuteczny system ochrony danych osobowych? Jakie korzyści przynosi systemowe podejście do ochrony danych osobowych? Udostępniania dokumentacji medycznej a dane osobowe.

Abstract

How to build an effective protection system of personal data? What are the benefits of system approach to data protection? Sharing of medical records vs. personal data.

Dlaczego system?

Często zostaje mi zadane pytanie dlaczego posługuję się terminem „system". W ustawie o ochronie danych osobowych nie ma o tym mowy. W rozporządzeniach wykonawczych jest mowa o systemie, ale w ujęciu systemu informatycznego, nie zaś systemu ochrony danych osobowych. Najczęściej odpowiadam, że brak podejścia systemowego to jeden z większych błędów konstrukcji tych dokumentów. Łatwiej w odniesieniu do norm ISO jest mówić o systemie, który w cyklu Deminga należy: zaplanować, ustanowić, wdrożyć, utrzymywać

Jak to się ma w kontekście systemu ochrony danych osobowych? Zaplanować - poprzez obiektywne spojrzenie na procesy realizowane prze Administratora Danych. Celowo użyłem słowa „obiektywne", gdyż na tym etapie często stwierdzamy, że opisywany system wymaga dopracowania. W procesie klasyfikacji aktywów informacyjnych Administrator Danych na tym etapie uświadamia sobie jakie zbiory faktycznie przetwarza i w jakim zakresie. Wymagane jest zatem zaplanowanie pewnych działań, które obejmą ochroną stan faktyczny lub ograniczą zakres przetwarzania w przypadku, gdy jest on zbyt duży. W procesie planowania często diagnozuje się zbyt duże rozproszenie zbioru w różnych systemach IT czy też przetwarzaniu tradycyjnym.

Ustanowić - poprzez opisanie systemu zgodnie z wymogami prawa, tj. Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym, upoważnieniami, ewidencją upoważnień, ewidencją udostępnień, powierzania przetwarzania. Proces ustanawiania systemu porządkuje procesy wokół przetwarzania danych osobowych. Dodatkowo przygotowuje podmiot na działania przyszłe, np. outsourcing.

Wdrożyć - znaczy mieć pewność, ze nasz system we wszystkich warstwach przetwarzania danych osobowych jest przemyślany, i nie diagnozujemy w nim słabego ogniwa. Oznacza to, że pozostałe ryzyko szczątkowe zostało świadomie zaakceptowane. Poprzez wszystkie warstwy rozumiemy warstwę elektronicznego przetwarzania danych (IT), warstwę organizacyjną (obszary przetwarzania) oraz zasoby ludzkie upoważnione do przewarzania jak i podmioty, którym dane do przetwarzania powierzamy. W dobrze zbudowanym systemie ochrony danych osobowych osoby uczestniczące w procesach przetwarzania powinny mieć poczucie komfortu, nie zaś dyskomfortu wynikającego najczęściej z lęku przed nieznanym.

Utrzymywać - poprzez świadomość konieczności udoskonalania systemu oraz dostosowywania go do zmieniającej się rzeczywistości w zakresie wymogów prawa, czy wymagań biznesowych. W cyklu Deminga ważnym aspektem jest gotowość do ciągłego doskonalenie systemu. W tej chwili padło słowo-klucz: „ciągłość". Jutro nie daje nam gwarancji, że będzie to „dziś, tyle że jutro". Nie jesteśmy w stanie przewidzieć co będzie jutro, ale możemy być przygotowani na działania naprawcze naszego systemu. I taki też jest sens utrzymywania sprawnego systemu ochrony danych osobowych.

Systemowe podejście do ochrony danych osobowych wydaje się najbardziej właściwe. Każde inne, odrzucające fundament cyklu Deminga PDCA (Plan, Do Check, Act) wydaje się być podejściem pasywnym, tj. biernym spełnieniem pewnych wymogów bez podejścia podmiotowego. Ja zawsze proponuję podejście do danych osobowych jako bardzo ważnego aktywu funkcjonowania podmiotu. W sektorze medycznym to podejście wydaje się mieć szczególne uzasadnienie. W zbliżającej się europejskiej reformie ochrony danych osobowych używa się dwóch bardzo ważnych zwrotów, dwie idee, które jasno wskazują kierunek zmian.

Privacy be design – idea odnosząca się do budowania systemów informatycznych, sugerująca by rozważanie prywatności przetwarzania danych osobowych rozpocząć na etapie tworzenia systemu lub nawet jego koncepcji. Dużo łatwiej jest planując proces osadzić go w istniejącej rzeczywistości obowiązku szanowania i ochrony prywatności niż odłożyć to do czasu dodatkowych wymagań wdrożeniowych czy też naprawczych.

Privacy by default – idea mówiąca o ochronie danych jako wartości domyślnych, nie marginalizowanej w procesach biznesowych.

Udostępnianie dokumentacji medycznej a ochrona danych osobowych

W jaki sposób udostępnić dokumentację medyczną bez sprawnego systemu danych osobowych? Z punktu widzenia Administratora Danych osobowych to bardzo ważne pytanie. Dokumentacja medyczna stanowi szczególną kategorię danych osobowych. Regulacje prawne dotyczące prowadzenia i udostępniania dokumentacji medycznej zawierają przepisy m. in. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania nie określają precyzyjnie formy upoważnienia do uzyskania dokumentacji medycznej. Z pomocą przychodzi nam system ochrony danych osobowych, gdzie powinna być jawna procedura postępowania w takim przypadku. Przepływ danych obejmuje wszystkie etapy procesu, począwszy od aspektu poinformowania osoby, której dane dotyczą poprzez wypracowanie formularza oświadczenia pacjenta o upoważnieniu, a skończywszy na obowiązku odnotowania faktu udostępnienia dokumentacji.

Dodatkowo trzeba mieć na uwadze, że osoba upoważniająca inną osobę do udostępnienia jej dokumentacji medycznej winna uczynić to zgodnie z zasadami wynikającymi z ogólnych przepisów o pełnomocnictwie, określonych w art. 98 i następne Kodeksu cywilnego.

Podsumowanie

Dane osobowe w sektorze medycznym podlegają ochronie niezależnie od tego, że mogą istnieć zbiory danych, które są zwolnione z rejestracji w GIODO. Dane medyczne stanowiące szczególną kategorię danych osobowych, podlegające szczególnej ochronie. Opisywane, systemowe podejście do ochrony danych osobowych daje gwarancję jakości ich przetwarzania. Jasne reguły dla osób przetwarzających dane, podziału ról i upoważnień do przetwarzania oraz jawne procesy przetwarzania w systemach informatycznych oraz w sposób tradycyjny. Dobrze zbudowany, sprawny system z pewnością zostanie zauważony przez pacjentów (klientów), dla których są to informacje poufne. Obowiązek przestrzegania prawa w zakresie danych osobowych osadzony w sprawny system ochrony danych osobowych można obrócić w atut biznesowy, czego Państwu serdecznie życzę.