Audyt RODO – czym jest w istocie

Zamierzasz wykonać audyt RODO samodzielnie lub zamówić usługę u zewnętrznego wykonawcy? Dowiedz się na czym ta usługa tak naprawdę polega i za co ewentualnie zapłacisz.

Kiedy wykonano pierwsze audyty ochrony danych osobowych?

Na samym wstępie – ważny komunikat: wzór audytu RODO nie znajduje się w Sevres pod Paryżem. Nie został też zapisany w żadnych przepisach powszechnie obowiązującego prawa.

Metodologia i praktyka audytów ochrony danych osobowych, to bardzo młoda sfera usług doradczych.

Obecnie słowo audyt większości przedsiębiorców kojarzy się z audytem finansowym. I nie ma w tym nic dziwnego. Audyt finansowy jestnajdłużej praktykowany i najlepiej wystandaryzowany.

Aby dobrze oddać skalę czasową należy zauważyć, że audytem finansowym branża doradcza zajmuje się od wieku XIX, a więc… już ponad dwa stulecia!

Audyt ochrony danych osobowych to usługa, która jest rozwijana dopiero od połowy lat dziewięćdziesiątych ubiegłego wieku. Jak łatwo policzyć – to nieco ponad 20 lat, a więc jedno zero mniej na osi czasu!

Dopiero pojawienie się Dyrektywy 95/46/WE (poprzedniczki RODO), a w Polsce ustawy o ochronie danych osobowych z 1997 roku, spowodowało zainteresowanie biznesu i sfery publicznej audytem pod kątem danych osobowych.

O pierwszych takich audytach, możemy więc mówić w Polsce od roku 1997.

Na przestrzeni następnych lat powstała pewna (niewielka) ilość firm koncentrująca swoją działalność na ochronie danych osobowych. Te organizacje miały czas i zasoby na stopniowe udoskonalanie metodyki oraz sposobów prezentowania wniosków płynących z przeprowadzonego audytu.

RODO i co dalej?

RODO stosowane jest od 25 maja 2018 roku i spowodowało konieczność przemodelowania podejścia do audytu ochrony danych osobowych. System audytu oparty na weryfikacji przepisów ustawy o ochronie danych osobowych z 1997 roku musiał zostać poważnie zmodyfikowany. Oczywiście wcześniejsze doświadczenia procentują i są doskonałą bazą do budowy metodologii zgodnej z RODO.

Do czego nam potrzebny audyt RODO?

Audyt RODO porównam do zaawansowanego skanu tkanek miękkich, jakim jest rezonans magnetyczny.

Jeśli chcemy podjąć skuteczne leczenie (np. uszkodzonego stawu), to nie da się tego zrobić bez dobrej diagnozy. A tę można postawić tylko dysponując odpowiednio przeprowadzonym badaniem.

Prawidłowo wykonany audyt RODO zobrazuje nam, jakie dane osobowe i w jaki sposób przetwarzamy w naszej organizacji. Będzie podstawą do podjęcia kolejnych decyzji oraz sposobu wdrożenia RODO.

Bez dobrze postawionej diagnozy może okazać się, że cała kosztowna terapia (wdrożenie) przyniesie więcej szkód, niż korzyści.

Jest jeszcze jedna duża wartość dodana posiadania raportu z audytu. Jedno z pierwszych pytań, które zadają inspektorzy UODO w toku kontroli, brzmi: „na jakiej podstawie ustalili Państwo ten stan faktyczny – czy możemy zobaczyć jakiś raport z audytu?"

Niezależnie wiec od tego czy działamy własnymi siłami (wewnętrznie), czy też szukamy zewnętrznego dostawcy – zanim zabierzemy się za wdrażanie RODO – najpierw postawmy precyzyjną diagnozę!

Na jakie pytania powinien dać odpowiedź audyt RODO?

Idąc tokiem medycznych skojarzeń – jeśli mamy dobrze wykonane zdjęcie ze specjalistycznym opisem (raport z audytu), to nie pozostaje nam nic innego, jak wybrać metodę leczenia (wdrożenia ogólnego rozporządzenia o ochronie danych).

Prezentacja raportu z audytu powinna dać nam odpowiedzi na kluczowe pytania, jak w szczególności:

1) Jakie działania na danych osobowych mają miejsce w naszej organizacji (więcej – w kolejnych akapitach),
2) Czy procesy przetwarzania danych mają oparcie w przesłankach legalności RODO?
3) Czy nie przetwarzamy zbyt dużo danych osobowych (zasada minimalizacji)?
4) Czy obecnie stosowane rozwiązania są skuteczne i działają?
5) Czy musimy powołać Inspektora Ochrony Danych?
6) Czy stosujemy tzw. profilowanie kwalifikowane?
7) Czy nasi pracownicy znają obecnie funkcjonujące procedury i jaki jest poziom ich świadomości swoich obowiązków?
8) Do jakich zewnętrznych podmiotów transferujemy dane osobowe (wykaz powierzeń przetwarzania danych oraz udostępnień danych).
9) Czy transfery danych do zewnętrznych podmiotów mają oparcie w postaci umów powierzenia lub przesłanek legalności udostępnienia danych?
10) Czy stosujemy prawidłowe obowiązki informacyjne?
11) Czy stosujemy prawidłowe klauzule zgód?

12) Czy kontrolujemy zabezpieczenia informatyczne i techniczne (o tym szerzej w kolejnych akapitach)?

13) Czy nasza organizacja ma opracowaną strukturę systemu ochrony danych? Czy każdy wie, za co odpowiada w ramach tej struktury?

14) W jaki sposób realizowane są prawa osób, których dane są przetwarzane?

15) Czy pracownicy wiedzą, jak zachować się w razie naruszenia ochrony danych?

16) Czy jesteśmy w stanie wykazać przestrzeganie przepisów przez naszą organizację (zasada rozliczalności).

Audyt to nie jest wdrożenie

Warto mocno rozdzielić dwa obszary: obszar audytu, który wcześniej porównałem do badania rezonansem magnetycznym oraz obszar wdrożenia, który możemy porównać do podjęcia leczenia.

Żeby zobrazować to przykładami – audyt może zawierać precyzyjnie zmapowane procesy. Ale nie będzie zawierał samego Rejestru Czynności Przetwarzania.

Raport z audytu może zawierać wskazanie, że brakuje klauzul informacyjnych w miejscach X, Y i Z. Ale nie będzie on uwzględniał treści samych klauzul informacyjnych.

Raport może zawierać rekomendację dotyczącą wdrożenia procedury DPIA, ale nie będzie uwzględniał samej procedury.

Audyt ma za to umożliwić lepsze poznanie własnej organizacji i stanowić punkt wyjścia przed rozpoczęciem wdrożenia.

Często podczas omawiania raportu z audytu, może okazać się, że wspólnie znajdziemy optymalny sposób wdrożenia w organizacji.

Mapowanie procesów, a audyt RODO

Kolejny ważnym elementem audytu RODO jest mapowanie procesów przetwarzania danych osobowych.

Dobrze przygotowana mapa procesów, to fundament wiedzy o tym co dzieje się z danymi osobowymi w naszej organizacji.

Jeśli audyt obejmuje też mapowanie procesów to dowiemy się między innymi:

1) Na jakiej podstawie prawnej przetwarzamy dane osobowe w każdym z procesów,
2) Komu są one powierzane,
3) Czy są transferowane do państw trzecich
4) A także wiele innych istotnych informacji. Jakich? Samemu mapowaniu procesów już poświęciliśmy odrębny artykuł, zapraszam do lektury – Rejestr Czynności Przetwarzania – mapowanie procesów

Mapa procesów pozwoli nam też na sprawne przygotowanie Rejestru Czynności Przetwarzania, które jest jedymn z podstawowych elementów wdrożenia RODO.

Audyt RODO bez mapowania procesów – nie jest audytem nieprawidłowym. Jak już wskazałem na początku artykułu – nie istnieje uniwersalny wzór audytu RODO.

Niemniej jednak w audytach, które prowadzimy, mapowanie procesów stanowi jeden z najbardziej czasochłonnych elementów.

Jeśli decydujemy się na wersję audytu bez mapowania procesów – powinno to też znaleźć odzwierciedlenie w cenie audytu.

Sposób prowadzenia audytu – mailowe checklisty czy audyt na miejscu?

Zbieranie informacji potrzebnych do przygotowania raportu, może odbywać się w różny sposób. Wyróżnię 3 różne praktyki w tym zakresie.

1) Audyt „na żywioł". Jest to metoda niebazująca na usystematyzowanych i kompletnych „checklisty", bez ustalonej metodologii. W takiej sytuacji audytor przyjeżdża do siedziby i zbiera informacje bezpośrednio od pracowników. Zaletą takiej formy zbierania informacji jest konieczność większej inicjatywy ze strony audytora. To audytor zbiera informacje, a później na ich bazie przygotuje raport.

   Jeśli jednak audytor nie ma przygotowanych checklist, oznacza to, że każdy audyt może być trochę inny. Jeśli audytor będzie miał akurat gorszy dzień, to może zapomnieć o zadaniu ważnych pytań i tym samym istotne wnioski nie znajdą się w raporcie.

   Audyty nie bazujące na checklistach są przeważnie wykonywane przez osoby zajmujące się RODO, działające na własnych rachunek lub przez nowe organizacje, które jeszcze nie wypracowały własnej metodologii realizacji usług.

2) Audyt usystematyzowany, „DIY - zrób to sam". Metoda bazująca na usystematyzowanych checklistach, których wypełnianie zostaje „przerzucone" na audytowanych pracowników.

   Wiele razy w toku naszej pracy spotkaliśmy się z audytami prowadzonymi zwłaszcza przez duże korporacje, które polegały na wysyłce checklist do audytowanych pracowników.

   Taka forma audytu świadczy o tym, że podmiot audytujący dopracował się już pewnej metodologii swoich działań. Może ją też zmieniać i udoskonalać.

   Ma jednak dwie istotne wady:

a. Niższa wiarygodność wyników audytu. Bazując tylko i wyłącznie na checklistach, ograniczamy do minimum bezpośredni element audytu. Tracimy przez to całkowicie „element zaskoczenia" i możliwość identyfikacji niezgodnych z RODO obszarów, które nie zostaną wskazane przez pracownika.

b. Czasem ze względu na chęć zaprezentowania się z jak najlepszej strony (mało kto lubi wskazywać na uchybienia we własnej komórce organizacyjnej), a czasem z braku odpowiedniej wiedzy, odpowiedzi udzielone przez audytowanych przez nas w ten sposób pracowników mogą pozostawiać wiele do życzenia. Mało kto w statystycznej organizacji zna się przecież na pojęciach takich jak „powierzenie", „profilowanie", czy „szczególne kategorie danych".

c. Ukryte koszty. Przerzucając ciężar realizacji audytu na pracowników, odciągamy ich na wiele godzin od realizacji ich codziennych obowiązków. Strata będzie tym większa, jeśli checklista będzie zawierała mało precyzyjne pytania. Warto uwzględnić ten koszt przy kalkulacji, który rodzaj audytu sprawdzi się najlepiej w naszej organizacji. Dodatkowo, audyty RODO „DYI – zrób to sam" są powszechnie znienawidzone przez pracowników. Audytowani pracownicy

mają często poczucie przerzucania na nich realnego ciężaru wykonania audytu, obawiają się też (zazwyczaj słusznie!), że nie są osobami kompetentnymi do udzielenia odpowiedzi na dane pytanie.

3) Audyt „systematycznie i bezpośrednio". Metoda polegająca na działaniu na usystematyzowanych kwestionariuszach wypełnianych przez audytora.

   Forma checklist wypełnianych na miejscu przez audytorów jest według mnie formą optymalną z perspektywy Klienta. To audytor bierze na siebie ciężar wyjaśniania pojęć z formularza i jego uzupełnienie.

   Zachowujemy też „element zaskoczenia". Nikt tak jak osoba z zewnątrz (ekspert firmy doradczej lub niezależny wewnętrzny audytor) nie jest w stanie obiektywnie zidentyfikować niezgodności z audytowanym obszarem.

   Dodatkowo, formularze gwarantują pewną powtarzalność i możliwość stałego udoskonalania procedur audytowych.

   Oczywiście są też wady takiego rozwiązania – z uwagi na większe zaangażowanie audytorów – takie rozwiązanie może być też droższe, niż audyt bazujący na zdalnie wysyłanych informacjach.

Jeśli zamierzamy prowadzić audyt wewnętrzny lub dokonać wyboru podmiotu audytującego – warto od razu ustalić preferowaną przez nas formę realizacji audytu.

Czy audyty RODO różnych dostawców są ze sobą kompatybilne?

Idealna sytuacja mogłaby wyglądać następująco. Jesteśmy audytowani przez spółkę Y. Na zakończenie otrzymujemy zwięzły raport, dzięki któremu dokładnie wiemy, co jest potrzebne, aby zapewnić nam zgodność z RODO.

Pytamy spółkę Y o koszt wdrożenia, który niestety okazuje się być poza naszym zasięgiem.

Rozpoczynamy więc poszukiwanie innego podmiotu. Znajdujemy spółkę Z, która zrealizuje wdrożenie w bardziej przystępnej kwocie. Spółka Z w całości opiera się na raporcie przygotowanym przez spółkę Y.

Wdrożenie przebiega szybko i sprawnie.

To niestety tylko idealna wizja, która byłaby możliwa do realizacji, gdyby każdy raport składał się z podobnych elementów.

W praktyce sytuacja przypomina niestety nieco bardziej tę znaną ze sfery IT, kiedy często nowy wykonawca woli wykonać system od podstaw, niż wdrażać się w prace prowadzone przez poprzedników.

Czas pokaże co wydarzy się dalej. Jeśli uda się wypracować pewne wspólne rynkowe standardy – na pewno będzie to z korzyścią dla Klientów.

Na ten moment, to co możemy zrobić to samodzielnie ustalić co dokładnie otrzymamy w ramach usługi nazwanej raportem z audytu.

Audyt RODO, a sfera IT

W przeciwieństwie do poprzedniego systemu, czyli ustawy ochronie danych osobowych z 1997 roku i Rozporządzenia MSWiA w sprawie dokumentacji i zabezpieczeń technicznych – RODO jest aktem prawnym „informatycznie obojętnym".

Było to jak najbardziej działanie celowe. Prawnicy pracujący nad treścią RODO zdawali sobie sprawę z tego, że postęp w sferze IT bardzo szybko wyprzedzi każde regulacje prawne.

Przykładowo: RODO nie zastrzega składni hasła czy częstotliwości jego zmiany.

Każdy administrator danych sam decyduje o tym, jakieś środki zabezpieczeń IT będą adekwatne do zabezpieczenia jego infrastruktury.

Nasze podejście do obszaru IT jest następujące. Rekomendujemy zbadanie poziomu bezpieczeństwa technicznego w organizacji – ale sprawami IT najlepiej zajmą się firmy stricte informatyczne lub wewnętrzne działy IT.

Dlatego my w Lex Artist, w ramach audytu RODO sprawdzamy obszar IT wyłącznie pod kątem, czy Administrator danych podjął jakiekolwiek działania zmierzające ku weryfikacji stosowanych zabezpieczeń. Sprawdzamy czy zabezpieczenia zostały wylistowane i czy możemy uznać obszar IT za odpowiednio zaadresowany.

Prezentacja raportu

Raport z audytu może być wielostronicowym dokumentem. Jednak nie wszyscy pracownicy Administratora danych, będą mieli czas na jego precyzyjną analizę.

Dlatego niezwykle ważna jest zwięzłe zaprezentowanie Zarządowi kluczowych wniosków i obserwacji płynących z audytu. Możemy też podzielić prezentację na poszczególne działy audytowanej organizacji, np. kadry, marketing etc.

Warto od razu ustalić z firmą audytującą, czy w ramach usługi otrzymamy również zaprezentowanie raportu w naszej siedzibie.

Jak zweryfikować doświadczenie audytorów?

Jeśli zdecydujemy się na realizację audytu RODO za pośrednictwem zewnętrznej firmy, warto zastosować więcej niż jedno kryterium wyboru – 100% cena.

Jednym z nich powinno być doświadczenie. Tylko jak w nowej, „postRODOwskiej" rzeczywistości ocenić obiektywnie to kryterium?

Od 25 maja 2018 nie działa jawny rejestr Administratorów Bezpieczeństwa Informacji. Do tej pory prowadzony przez Regulatora rejestr mógł pomóc zweryfikować doświadczenie audytora.

Mogliśmy sprawdzić w ilu organizacjach (i czy w ogóle) pełni funkcję ABI, a tym samym mieć pewne pojęcie o jego praktycznym doświadczeniu.

Dzisiaj rejestr IOD nie jest jawny, więc pozostają nam inne formy sprawdzenia doświadczenia. Ja zalecam w szczególności:

1) Pochwalenie się referencjami dotyczącymi wdrożeń i audytów przed 25 maja 2018. W ten sposób nie bierzemy pod uwagę dostawców, którzy dopiero uczą się audytu ochrony danych osobowych,
2) Sprawdzenie jak długo istnieje firma realizująca dla nas audyt. Jeśli powstała w 2018 roku, to wygląda na to, że powstała właśnie z okazji RODO. Nie ma w tym nic złego – ale nie spodziewajmy się dużego doświadczenia po audytorach.
3) Weryfikacja specjalizacji podmiotu audytującego. Jeśli obok RODO w liście specjalizacji znajdziemy: prawo karne gospodarcze, prawo energetyczne, prawo pracy, własność intelektualną, prawo handlowe (..) i 10 innych specjalizacji... to z całą pewnością ten podmiot nie specjalizuje się w ochronie danych osobowych.

Koszt audytu vs. stopień szczegółowości audytu

Dopiero wiedząc na czym dokładnie polega audyt RODO i z jakich elementów się składa, możemy zestawić ze sobą i porównać oferty różnych dostawców.

Proponuję krótką checklistę, która pozwoli nam ocenić usługę oferowaną przez dostawcę pod kątem szczegółowości i stopnia zaawansowania:

1) Audyt będzie prowadzony w naszej siedzibie (TAK/NIE)
2) Metodologia realizacji audytu bazuje na checklistach, które wypełnia audytor (TAK/NIE)
3) Raport z audytu zostanie zaprezentowany w siedzibie (TAK/NIE)
4) W ramach audytu zostanie zbadany poziom świadomości pracowników pod kątem ochrony danych osobowych (TAK/NIE)
5) Raport będzie zawierał zmapowane procesy przetwarzania danych (TAK/NIE)

Podsumowanie

Mimo, że branża audytu ochrony danych osobowych, nie jest jeszcze tak wystandaryzowana jak branża audytu finansowego, to możemy wyróżnić pewne elementy wspólne dla każdego audytu RODO.

Im lepiej znamy usługę, którą zamawiamy tym łatwiej będzie nam dokonać optymalnego dla naszej organizacji wyboru.

Jeśli realizujemy audyt samodzielnie – zastosujmy się do poniższych wytycznych, którymi kierują się również profesjonalne firmy doradcze:

1) Wyraźnie oddzielamy etap audytu od etapu wdrożenia.
2) Działania audytowe kończymy przygotowaniem pisemnej wersji raportu.
3) Raport zawiera ocenę kluczowych z perspektywy RODO obszarów (por. akapit „na jakie pytania powinien dać odpowiedź audyt RODO").
4) Raport prezentujemy w formie krótkiej prezentacji (kluczowe wnioski).
5) Dopiero po zaprezentowaniu raportu i ustaleniu z Zarządem sposobu implementacji, przechodzimy do kolejnego etapu - wdrożenia procedur RODO

Autor artykułu:

Przemysław Zegarek

Źródła:

- 10 letnie doświadczenie pełnienia funkcji ABI/IOD lub wsparcia ABI/IOD w ponad 100 organizacjach. Kilka tysięcy godzin szkoleniowych (w tym szkoleń dla ABI) i ponad 500 wdrożeń systemów ochrony danych osobowych,
- Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, 1669).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych).