RODO audyt procesora – jak to zrobić z głową?

W jaki sposób audytować procesora? Kiedy audytować? Co zrobić, żeby nie zniechęcić do siebie naszych kontrahentów? Zapraszam do lektury!

Auditor po łacinie znaczy: słuchający

Audyt ochrony danych osobowych, to bardzo młoda dziedzina. Dopiero się rozwija i wypracowuje własne standardy.

Najdłuższą tradycję audyt ma w dziedzinie finansów i rachunkowości. Tutaj wypracowano wieloletnią praktykę sięgającą wieku XIX.

Jednak pierwsze audyty finansowe prowadzili już starożytni rzymianie. Stąd pochodzi słowo audyt: łac. *auditor* – słuchacz, słuchający.

Rzymski audyt polegał na przesłuchiwaniu urzędników odpowiedzialnych za finanse i sprawdzaniu czy nie doszło do nieprawidłowości.

Nikt nie lubi być przesłuchiwany. Nikt nie lubi być również audytowany. Niezależnie od tego czy jesteśmy audytowanym czy audytującym, sam proces audytu będzie budził pewne emocje.

Im większa będzie nasza pewność siebie i doświadczenie, tym poziom stresu będzie mniejszy.

Jako audytujący – musimy znać pewne zasady i reguły, które ułatwią nam współpracę z audytowanym podmiotem.

Jeśli to my jesteśmy audytowani – kluczowa będzie znajomość systemu ochrony danych osobowych w naszej organizacji.

Chcę, aby niniejszy artykuł pomógł zarówno audytującym, jak i audytowanym. Im większa wiedza, tym mniejszy będzie poziom stresu w trakcie audytu.

Audyt nie musi polegać na szukaniu winnych i czepianiu się nieistotnych szczegółów. Działanie audytowe może stać się okazją do nauczenia się czegoś nowego dla obu stron.

Czy audyt procesora jest niezbędny dla zgodności z RODO?

Na początek krótkie przypomnienie. Procesor (inaczej: podmiot przetwarzający) to organizacja, która w naszymi imieniu przetwarza dane osobowe, którymi administrujemy.

Procesorami będą na przykład: firmy z branży IT, firmy organizujące dla nas działania marketingowe, biura rachunkowe etc.

Zapisy dotyczące audytu procesora są rozrzucone w różnych miejscach RODO. Jedynym przepisem bezpośrednio traktującym o audytowaniu procesorów jest art. 28 ust. 3 pkt. h).

Powyższy przepis stanowi, że procesor musi umożliwić administratorowi prowadzenie działań sprawdzających: audytów lub inspekcji.

Nie znajdziemy w RODO przepisu, który powie nam wprost, że audyty procesorów są konieczne i należy je prowadzić z określoną częstotliwością i w konkretny sposób.

Poniżej znajduje się lista przepisów Ogólnego rozporządzenia o ochronie danych osobowych, które w sposób pośredni lub bezpośredni odnoszą się do audytu procesora:

- art. 5 ust. 2 zasada rozliczalności
- art. 24 obowiązki ADO – odpowiednie środki techniczne i organizacyjne
- art. 28 ust. 3 pkt. h) „(procesor) (…) umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.”
- art. 39 ust. pkt b) audyty prowadzone przez IOD

Przepisy ogólne to np. zasada rozliczalności. W jaki sposób wykażemy, że zadbaliśmy o to, aby nasze dane osobowe były bezpieczne, jeśli nie zweryfikowaliśmy naszych dostawców (procesorów)?

Poza samymi przepisami, warto zwrócić też uwagę na powszechną praktykę, interpretacje i poradniki RODO wydawane przez regulatorów w UE.

Praktyka oraz regulatorzy idą zdecydowanie, w kierunku rekomendowania, wdrożenia pewnego poziomu kontroli nad procesorami (czyli audytu).

Jeśli pracujemy w dużej grupie kapitałowej, to istnieje bardzo duże prawdopodobieństwo, że nasza centrala poprosi nas o przedstawienie dowodów na to, że audytujemy swoich dostawców.

Jeśli nie poprosi nas o to bezpośrednio centrala, to możliwe, że zleci ona audyt RODO zewnętrznej firmie audytorskiej.

W jednym i drugim przypadku z prawdopodobieństwem graniczącym z pewnością, możemy spodziewać się pytania, o to w jaki sposób audytujemy naszych procesorów?

Dociekliwy audytor poprosi nas również o dowody świadczące o tym, że audyty faktycznie mają miejsce.

Jeśli pracujemy w małej organizacji i świadczymy usługi na rzecz dużych korporacji, to sytuacja wygląda dość podobnie.

Nasz korporacyjny klient może poprosić nas o wskazanie w jaki sposób i komu podpowierzamy dane osobowe, których jest administratorem.

Podsumowując – RODO nie mówi wprost o konieczności audytu procesora, niemniej jednak, możemy przyjąć, że pewna kontrola nad procesorami jest absolutnie niezbędna.

Musimy więc posiadać procedury audytu procesora i co więcej – musimy stosować je w praktyce.

Jakie są korzyści i trudności związane z audytem procesora?

Część praktyczną zaczniemy od krótkiej analizy korzyści oraz trudności związanych z audytem procesora.

Korzyść	**Trudność**
Minimalizujemy ryzyko związane z transferem danych do podmiotów zewnętrznych	Audyt może być czasochłonny
Mamy czym się „pochwalić" na wypadek kontroli Regulatora czy audytu wewnętrznego	Audyty mogą zniechęcać do nas naszych dostawców
Zapewniamy 100% zgodności z RODO	Brakuje nam know – how potrzebnego do realizacji audytu

Warto przyjrzeć się szczególnie rubryce z trudnościami. Wdrażając procedury audytowe, możemy przygotować je w taki sposób, żeby zminimalizować trudności.

Jak to zrobić? O tym napiszę w kolejnych akapitach.

Jeśli audytuję procesora to czy potrzebuję jego zgody w umowie powierzenia?

Tak postawione pytanie pokazuje, że system ochrony danych osobowych jest pewną spójną całością. Jeśli chcę realizować audyty procesora, to warto zastrzec odpowiednią ich formę od razu na etapie podpisywania umowy powierzenia.

To co warto uregulować w umowie powierzenia, to w szczególności:

- **z jakim wyprzedzeniem Administrator zgłasza chęć wykonania audytu?**
- **kto pokrywa koszty częstych audytów?**
- **w jakich nieprzekraczalnych terminach procesor udostępnia administratorowi żądane informacje?**
- **jakie uprawnienia daje Administratorowi stwierdzenie istotnych uchybień w toku audytu?**

Warto podkreślić dwie kwestie:

1) Zbyt częste i zbyt szczegółowe audyty procesora to kosztowne działania. Zarówno dla administratora, jak i dla procesora. Jeśli to my jesteśmy procesorem i obawiamy się zbyt częstych audytów naszego kontrahenta – możemy od razu na etapie podpisywania umowy

powierzenia zastrzec, że dodatkowe koszty związane z obciążeniem czasowym procesora podczas audytu pokryje administrator danych.

2) Warto też od razu wprost ustalić, co dzieje się ze współpracą w przypadku wykrycia dużych nieprawidłowości. W tym przypadku audyt procesora może okazać się podstawą do podjęcia ważnej decyzji biznesowej (np. zakończenia współpracy).

Oczywiście jeśli nie określiliśmy precyzyjnie w umowie powierzenia kwestii związanych z audytem procesora, to na mocy samych przepisów RODO i tak procesor będzie zobowiązany do współpracy.

- art. 28 ust. 3 pkt. h) „(procesor) (…) umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich."

Niemniej jednak, dobre zapisy w umowie powierzenia, stawiają nas w znacznie bardziej komfortowej sytuacji.

Co konkretnie możemy audytować?

Jako administrator danych, możemy zbadać każdy aspekt związany z przetwarzaniem powierzonych danych osobowych.

W Lex Artist te obszary grupujemy w filary. W ten sposób zaprezentuję przykładowe możliwości audytowe w każdym z filarów:

1) Legalność
    a. W obszarze legalności nie ma zbyt dużo działań do podjęcia. Jeśli jesteśmy administratorem, to my musimy zadbać o zapewnienie przesłanek legalności dla procesu.
    b. Umowy powierzenia z subprocesorami – czy je podpisano, jaka jest ich treść?
    c. Czy procesor prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania? Warto sprawdzić czy takie dokumenty nasz procesor w ogóle posiada.
    d. Możemy oprzeć się na oświadczeniu procesora, że dokumenty wdrożono. Możemy iść dalej i poprosić o ich kopie czy dotyczące nas fragmenty kopii.

       Pamiętajmy o tym, że domagania się od procesora np. całego rejestru kategorii czynności przetwarzania może stanowić dla niego naruszenie tajemnicy przedsiębiorstwa. Dlatego domagać się możemy tylko niektórych dokumentów, zwłaszcza tych dotyczących bezpośrednio współpracy z naszą organizacją.

2) Świadomość

a. Możemy zbadać czy pracownicy procesora wiedzą jak się obchodzić z powierzonymi danymi osobowymi.

b. W szczególności możemy sprawdzić ich ogólny poziom wiedzy (np. czy wiedzą czym są dane osobowe i ich przetwarzanie), albo na czym polega relacja administrator – procesor.

c. Możemy zweryfikować czy pracownicy procesora potrafią realizować w praktyce procedury raportowania o incydentach lub czy potrafią realizować prawa przysługujące osobom fizycznym.

d. Możemy też oprzeć się na samych deklaracjach procesora, że przeszkolił swój personel.

e. Możemy poprosić o „podkładkę" pod deklarację o szkoleniu – zaświadczenie lub certyfikat.

3) Zabezpieczenia

a. Możemy zapytać o wdrożenie procedur RODO u procesora. Takie procedury jak np. raportowanie o incydentach są szczególnie istotne w przypadku powierzeń przetwarzania danych.

b. Możemy zapytać o fakt wdrożenia polityk ochrony danych osobowych czy innych zabezpieczeń organizacyjnych.

c. Możemy zweryfikować zabezpieczenia IT (tutaj potrzebne będzie wsparcie informatyka z naszej strony).

d. Podobnie jak w przypadku świadomości – możemy uznać same oświadczenia procesora za wiarygodne i nie wnikać w ich prawdziwość. Możemy też poprosić o konkretne procedury czy sprawdzić zabezpieczenia IT na miejscu.

4) Regulator

a. Warto sprawdzić czy procesor wyznaczył inspektora ochrony danych. Oczywiście taki obowiązek nie zawsze istnieje, jednak fakt wyznaczenia IOD, zawsze możemy interpretować na korzyść procesora.

b. Jeśli nie wyznaczono IODa, sprawdźmy czy w kontrolowanym podmiocie w ogóle jest osoba, która deklaruje, że podjęła się odpowiedzialności za procesy przetwarzania danych osobowych.

Jeśli takiej osoby w ogóle nie ma – zdecydowanie powinna nam się zapalić „lampka ostrzegawcza".

5) Prawa osób

a. Jeśli procesor ma w naszym imieniu dopełniać obowiązki informacyjne czy realizować prawa osób, których dane są przetwarzanie – koniecznie sprawdźmy, czy robi to w prawidłowy sposób.

b. Sprawdźmy też czy ma do takich działań odpowiednie zasoby. Jeśli osób realizujących swoje prawa będzie dużo – procesor musi posiadać odpowiednio liczny i przeszkolony personel.

c. Jeśli to my jako administrator realizujemy prawa osób, to musimy mieć 100% pewności, że procesor niezwłocznie będzie nam przekazywał wszelkie pisma i maile.

Kogo audytować?

Kolejne istotne pytanie to kwestia tego, kogo poddawać audytowi. Jeden z naszych Klientów otrzymał zalecenie od centrali aby przeaudytować wszystkich swoich dostawców usług.

Szybka analiza systemu CRM wykazała, że dostawców jest… kilkanaście tysięcy.

Audyt kilkunastu tysięcy procesorów zająłby ogromną ilość czasu, którego potem zabrakłoby na inne filary związane z ochroną danych osobowych.

Jak więc poradzić sobie w sytuacji dużej ilości dostawców?

Najczęściej stosowane są dwa rozwiązania, przy czym można je ze sobą dodatkowo łączyć.

1) Metoda selekcji procesorów: wybieramy tylko tych dostawców, którzy przetwarzają największą ilość danych osobowych (w tym np. dane szczególnie chronione).

   Warto najpierw ustalić kryteria wyboru, a następnie audytować tylko wybranych dostawców usług.

2) Metoda próbkowania: dzielimy procesorów na różne grupy ryzyka, a następnie audytujemy kilku przedstawicieli każdej z grup.

Jak skutecznie audytować?

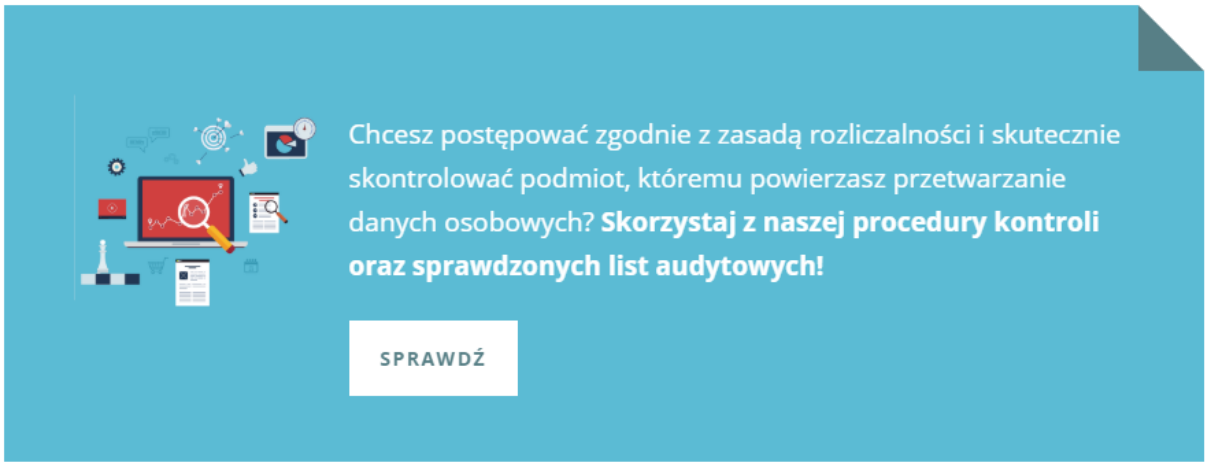
Skuteczny audyt wcale nie musi być bardzo długi i uciążliwy dla obydwu stron. Skutecznym narzędziem będą przede wszystkim checklisty audytowe.

Odpowiednio opracowane checklisty pozwolą na zweryfikowanie procesora w skuteczny sposób nawet poprzez audyt zdalny.

W praktyce, tak właśnie wygląda większość audytów procesora – zdalna wysyłka checklist i analiza zebranych informacji. W razie konieczności, poproszenie o dokumenty potwierdzające złożone w formie wypełnionych checklist oświadczenia.

Od czego więc zacząć? Przede wszystkim od przygotowania checklist z pytaniami dla audytu zdalnego.

Możesz zainspirować się naszymi listami audytowymi, możesz je zmodyfikować lub stworzyć je od podstaw.



Jeśli tworzysz własne pytania, z całą pewnością zwróć uwagę na następujące kwestie:

1) Unikaj zbyt dużego poziomu ogólności pytań.

Na przykład pytanie, o to czy procesor działa zgodnie z RODO, będzie zdecydowanie zbyt ogólne. Takie pytanie zdarzało się naszym klientom otrzymywać od audytujących podmiotów.

2) Unikaj zbyt dużego poziomu szczegółowości pytań

Zbyt szczegółowe pytania, również mogą skomplikować nam zadanie i utrudnić wyciągnięcie trafnych wniosków.

Na przykład prośba o przesłanie przez procesora kompletu dokumentacji ochrony danych osobowych wraz załącznikami to zdecydowanie zbyt dużo.

3) Pytaj o daty

   a. Pytanie o daty może się okazać bardzo skuteczne dla audytora. Jeśli zapytamy, o to czy miały miejsce szkolenia z zakresu RODO, to zapewne zawsze uzyskamy odpowiedź twierdzącą.

      Jeśli jednak poprosimy o daty i miejsce realizowanych szkoleń, może się okazać, że procesor nie jest w stanie wskazać ani precyzyjnej daty, ani miejsca szkolenia. A to już zdecydowanie ważny sygnał ostrzegawczy dla audytora.

4) Dopasuj checklistę do procesora – najlepiej przygotowując 2 lub 3 jej wersje.

a. Warto przygotować minimum dwie wersje audytu. Jedna wersja będzie audytem bardziej ogólnym i uproszczonym. Taką wersję adresujemy do procesorów, którzy przetwarzają mniej istotne dane osobowe w mniejszych ilościach, tym samym generując dla nas mniejsze ryzyka prawne.

b. Druga wersja audytu to audyt bardziej szczegółowy, przeznaczony dla naszych kluczowych partnerów biznesowych. Na przykład dla dostawców naszego systemu informatycznego, przetwarzającego dane kadrowe czy dla firm zajmujących się marketingiem, tworzących bazy Klientów etc.

Audyt stacjonarny

Bazując na przygotowanych checklistach, możemy również zdecydować się na audyt stacjonarny. Pamiętaj o tym, że wizyta audytowa u naszego dostawcy wygeneruje dużo czasu i zaangażowania po obu stronach.

Na audyty stacjonarne decyduj się tylko w przypadkach kluczowych powierzeń przetwarzania danych osobowych.

Inną sytuacją, która uzasadnia realizację audytu stacjonarnego, może być wyciek danych osobowych po stronie procesora.

Co zrobić w przypadku wykrycia uchybień w toku audytu?

Każdy audyt powinien zakończyć się przygotowaniem raportu. Z prowadzonych przez nas działań powinno coś wynikać.

Wnioski z audytu, oczywiście mogą być bardzo różne. Od stwierdzenia braku uchybień, aż po znalezienie uchybień tak poważnych, że mogą one uzasadniać zakończenie współpracy z procesorem.

I tu ważna uwaga: arsenał dostępnych nam środków, będzie w dużej mierze zależał od tego, jaka jest treść podpisanej przez nas umowy powierzenia.

Środki, które możemy zastosować znajdując nieprawidłowości, powinny być oczywiście adekwatne do skali uchybienia.

- **Wezwanie do usunięcia uchybień**

  Standardowo – najlżejszy środek. Pamiętajmy jednak o tym, aby na usuniecie uchybień dać konkretny i nieprzekraczalny termin. A po jego upłynięciu sprawdzić czy uchybienia faktycznie zostały usunięte.

- **Sankcje biznesowe**

Wezwanie do usunięcia uchybień możemy oczywiście wzmocnić sankcjami nieformalnymi. Na przykład zaprzestaniem zakładania nowych kont w systemie czy zamawiania kolejnych usług do czasu podjęcia przez procesora działań naprawczych.

Arsenał sankcji biznesowych jest oczywiście ogromny, i o ile działamy legalnie – możemy również w sposób „miękki" i nieformalny wzmocnić przekaz płynący z wezwania na usunięcia uchybień.

- **Rozwiązanie umowy o współpracy**

  Wyjątkowo poważne uchybienia, mogą skutkować nawet, rozwiązaniem umowy o współpracę. Oczywiście najlepiej, jeśli takie rozwiązanie jest wprost przewidziane w umowę ramowej lub w umowie powierzenia.

  Jeśli współpraca i tak nie układa się dobrze i szukamy pretekstu do jej zakończenia, to poważne naruszenia w kwestii przetwarzania danych osobowych, mogą bardzo znacząco ułatwić nam życie.

- **Kary umowne zastrzeżone w umowie powierzenia**

  Tutaj znów kluczowe będą odpowiednie zapisy w umowie powierzenia. Odpowiednie zapisy umożliwią nałożenie kar umownych na procesora, w przypadku znalezienia uchybień w toku audytu.

- **Sankcje cywilnoprawne związane z prawem zobowiązań**

  Oczywiście przepisy ogólne kodeksu cywilnego, także mogą mieć zastosowanie do uchybień związanych z przetwarzaniem danych osobowych.

  Powoływanie się na przepisy kodeksu cywilnego, może być awaryjnym wyjściem w sytuacji braku odpowiednich zapisów w umowie powierzenia.

- **Poinformowanie regulatora**

  Zawsze mamy taką możliwość, oczywiście skorzystanie z niej raczej nie pozostanie bez wpływu na nasze relacje z procesorem.

- **Zawiadomienie do prokuratury**

  To najbardziej skrajna sytuacja. Pamiętajmy jednak, że w myśl art. 107. ust. 1 Ustawy o ochronie danych osobowych:

  „Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch."

  Jeśli więc, np. wykryjemy, że procesor przekazuje powierzone mu dane osobowe np. naszej konkurencji, to z całą pewnością możemy pomyśleć o zgłoszeniu tego faktu do prokuratury.

Podsumowanie

Audytować procesorów nie tylko trzeba, ale też warto. Jeśli wykonamy czynności audytowe, minimalizujemy ryzyko trafienia na nierzetelnych dostawców usług.

Jeśli znajdziemy uchybienia u naszego procesora, zyskujemy też skuteczne narzędzie biznesowe przy ewentualnych negocjacjach, co do kształtu oraz ceny usługi.

W przypadku poddania naszej organizacji audytowi (wewnętrznemu lub zewnętrznemu), wykazanie naszej aktywności na polu audytu procesora, na pewno będzie bardzo pomocne.

Zakładając, że bazujemy do dobrych checklistach audytowych, te wszystkie korzyści uzyskamy relatywnie niedużym nakładem czasowym.

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).