Warszawa, dn. 14.09.2022 r.

Jak przygotować audyt RODO?

Zanim przejdę do sedna tematu, najpierw – tytułem przypomnienia i wstępu – chciałbym przypomnieć naszym Czytelnikom jak definiowany jest audyt. Będzie to dobry punkt wyjścia do dalszych rozważań będących przedmiotem niniejszego wpisu. Cytując zatem normę ISO 27000, audyt jest to systematyczny, niezależny i dokumentowany proces uzyskiwania dowodu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu. Audyt może być wewnętrzny lub zewnętrzny (wspomniana norma wymienia jeszcze coś co nazywa się audyt kombinowany, ale nim nie będziemy się zajmować).

Cel audytu

Skoro definicja jest już za nami, pora zastanowić się, dlaczego w ogóle mam robić audyt np. jako inspektor ochrony danych w obsługiwanej przeze mnie organizacji. Odpowiedzi na tak postawione pytanie może być wiele, bo i różne mogą być cele audytu. Na potrzeby niniejszego wpisu wskazać mógłbym na przykład takie:

- identyfikacja procesów przetwarzania danych osobowych,
- określenie sposobów przepływu danych osobowych w ramach poszczególnych procesów,
- ustalenie przesłanki zezwalającej na zbieranie danych osobowych zgodnie z obowiązującym prawem,
- weryfikacja realizacji zasad przetwarzania danych,
- sprawdzenie wypełniania obowiązku informacyjnego,
- ustalenie w jakim zakresie oraz w jakim celu dane osobowe są powierzane do przetwarzania do firm zewnętrznych, a także czy sporządzono i podpisano na te okoliczności stosowne umowy powierzenia,
- sprawdzenie sposobu przechowywania danych osobowych przetwarzanych w wersji papierowej,
- inwentaryzacja systemów służących do przetwarzania danych osobowych,
- weryfikacja procedur wykonywania kopii zapasowych,
- określenie sposobów nadawania uprawnień do systemów informatycznych,
- weryfikacja zabezpieczeń logicznych systemów służących informatycznych.

Na dobrą sprawę planowany przez nas audyt może zawierać wszystkie wskazane wyżej cele. Tak będzie na przykład wtedy, gdy robimy audyt przedwdrożeniowy RODO. Przy tego typu audycie musimy tak naprawdę poznać całą organizację od strony przetwarzanych przez nią danych osobowych (jakie dane osobowe, do czego są wykorzystywane, na jakiej podstawie prawnej, itd.).

Plan audytu

Do planu audytu możemy podejść w sposób autorski, ale… Po co to robić? Mamy przecież doskonałe narzędzie w tym zakresie w postaci normy ISO 19011. Spójrzmy zatem co ww. norma doradza w tym zakresie. Otóż wspomniany wyżej plan powinien uwzględniać:

- cele audytu, które mogą wynikać np. z priorytetów kierownictwa, wymagań prawnych, wymagań wynikających z zawartych umów, wyników poprzedniego audytu, itd.,
- zakres, czas trwania (harmonogram) audytu – może być uzależniony np. od wielkości i charakteru organizacji, która będzie audytowana,
- procedury audytu – w tym przypadku chodzi o ustalenie m.in. sposobu składania raportów do kierownictwa np. w przypadku wykrycia niezgodności,
- kryteria audytu, czyli stosowanie odniesień w stosunku do których określana jest zgodność np. mające zastosowanie polityki, procedury, wymagania prawne, normy. Jest to niezwykle istotne w kontekście opisywania w raporcie niezgodności,
- metody audytu – przykładowo mogą to być: przeprowadzanie rozmów, wypełnianie list kontrolnych i kwestionariuszy, dokonywanie przeglądu dokumentacji, itd.,
- wyznaczenie zespołu audytującego – wskazanie audytora wiodącego i członków zespołu audytowego w oparciu o kompetencje, podział zadań i ról, jeśli audyt realizowany jest przez więcej niż jednego audytora,
- wskazanie niezbędnych zasobów – czyli kwestie organizacyjne takie jak np. wyznaczenie osoby koordynatora, udostępnienie sali, dostęp do Internetu, itp.,
- procesy dotyczące postępowania z poufnością, bezpieczeństwem informacji, itp. – jeśli audyt przeprowadza firma zewnętrzna, najczęściej będzie to regulowane w umowie, niemniej audytor powinien podkreślić np. podczas spotkania otwierającego znaczenie zapewnienia poufności.

Jak widać, przygotowanie dobrego plan audytu wymaga trochę czasu, ale warto to zrobić, bo dzięki temu nasza praca będzie nieco łatwiejsza do zrealizowania na późniejszym etapie.

Schemat przeprowadzenia audytu

Wiesz już czym jest plan audytu? Świetnie, w takim razie opowiem Ci teraz jak może wyglądać schemat przeprowadzenia audytu. W tym zakresie również odwołam się do wspomnianej wyżej normy ISO 19011. Norma ta wyodrębnia trzy etapy realizacji audytu:

1. Przygotowanie działań audytowych, na które składają się:
   - przeprowadzenie przeglądu dokumentacji w ramach przygotowania do audytu np. analiza schematu organizacyjnego, analiza strony (stron) www i dostępnych tam dokumentów i innych informacji np. regulaminów, polityk prywatności, formularzy, itp.,
   - przygotowanie planu audytu, czyli doprecyzowanie terminów (dzień, godzina, czas trwania), wskazanie zakresu poprzez wskazanie działów, które mają być audytowane – (np. na bazie schematu organizacyjnego i wstępnych informacji),
   - przydzielenie pracy członkom zespołu audytowego, czyli podział zadań, o ile audyt realizuje więcej niż jedna osoba,
   - przygotowanie dokumentów roboczych takich jak np. listy kontrolne, formularze do zapisywania informacji.
2. Przeprowadzanie właściwych działań audytowych:

- spotkanie otwierające, czyli wprowadzenie do audytu polegające m.in. na potwierdzeniu planu audytu, jego celów, zakresu oraz kryteriów, przedstawieniu zespołu audytującego, itp.,
- szczegółowy przegląd dokumentacji pod względem kompletności, spójności, aktualności, itp.,
- zbieranie i weryfikacja informacji, przy czym istotne jest to, że tylko informacja możliwa do zweryfikowania może być zaakceptowana jako dowód z audytu, a ten ostatni powinien zostać zapisany. Należy zatem m.in. wskazać źródło informacji oraz dowód z audytu,
- opracowanie ustaleń z audytu, czyli wskazanie niezgodności, przy audycie ochrony danych osobowych ustalenia przedstawiane są w raporcie,
- przygotowanie wniosków z audytu – m.in. przegląd ustaleń, przygotowanie rekomendacji; przy audycie ochrony danych osobowych ustalenia przedstawiane są w raporcie,
- spotkanie zamykające, którego celem jest przedstawienie ustaleń z audytu oraz wniosków. Na gruncie audytu ochrony danych osobowych może to być spotkanie polegające na zaprezentowaniu najważniejszych tez raportu dla ścisłego kierownictwa audytowanej organizacji.

3. Przygotowanie i dystrybucja raportu z audytu.

Jak rozmawiać?

Poniżej garść porad w jaki sposób audytor może prowadzić wywiady audytowe:

- nie odgrywaj roli złego policjanta - postaraj się wzbudzić zaufanie pracowników
- poinformuj / wytłumacz, dlaczego jest przeprowadzany audyt, jaka jest Twoja rola jako audytora
- rób dokładne notatki, a w razie potrzeby doprecyzuj wszelkie wątpliwości
- umawiaj spotkania z osobami, które mają największą wiedzę na temat poszczególnych procesów zachodzących z organizacji
- przeanalizuj dokumentację! Nie bazuj tylko na rozmowach z pracownikami
- pamiętaj, że osoba, z którą prowadzisz rozmowę może nie wiedzieć co oznaczają takie zwroty jak: umowa powierzenia, podmiot przetwarzający, dlatego forma oraz sposób zadawania pytań jest bardzo istotny. Zadawaj proste pytania a zawroty terminologii prawniczej zastępuj takimi odpowiednikami, które będą zrozumiałe dla Twojego rozmówcy
- pamiętaj, że będziesz rozmawiał z osobami z różnym wieku i na różnych stanowiskach - dostosuj komunikację do rozmówcy
- unikaj przeprowadzania rozmów audytowych z pracownikami w obecności ich przełożonego

Jakie pytania zadawać? Kilka przykładów

O pytaniach audytowych można napisać pewnie osobny artykuł, więc tu ograniczę się do kilku prostych przykładów:

- Jakie dane zbierane są w konkretnym procesie?
- Jakie dokumenty/formularze wykorzystywane są w danym procesie?
- Jak długo przechowywane są dane w określonym procesie?

- Czy dane przekazywane są do podmiotów zewnętrznych?
- Czy z podmiotami, do których przekazywane są dane zostały podpisane umowy powierzenia?
- Czy i na jakim etapie spełniany jest obowiązek informacyjny w konkretnym procesie?
- W jaki sposób niszczone są dane?
- Czy zdarzyły się naruszenia w przeszłości? Czego dotyczyły - sprawdzamy: czy były zgłaszane, czego dotyczyły, jakie środki zostały wdrożone by zapobiec naruszeniom w przyszłości, wiemy też jakie szkolenia dla działu zaprojektować itd.

Raport z audytu – sposób opisywania niezgodności

Poniżej tabelka z moją propozycją opisywania niezgodności.

Niezgodność z przepisami	Niezgodność o krytycznym znaczeniu. W przypadku kontroli ze strony organu nadzorczego bądź roszczenia skierowanego przeciwko administratorowi skutki mogą mieć bardzo duże konsekwencje (kara finansowa, konieczność wypłacenia odszkodowania). Wystąpienie takiej niezgodności wiąże się najczęściej z całkowitym niedopełnieniem określonego wymogu prawa bądź naruszeniem przepisu.
Częściowa niezgodność z przepisami	Niezgodność o niewielkim znaczeniu i średnim ryzyku mającym wpływ na biznes. W przypadku jej materializacji skutki mogą mieć niewielkie konsekwencje dla administratora (wydawanie przez organ nadzorczy ostrzeżenia dotyczącego możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania, udzielenie upomnienia w przypadku naruszenia przepisów RODO przez operacje przetwarzania, nakazanie spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO). Wystąpienie omawianej niezgodności wiąże się najczęściej z problematyką interpretacyjną określonego przepisu albo naruszeniem wypracowanych zasad (dobrej praktyki)
Zalecenie	Propozycja usunięcia niezgodności, minimalizacji ryzyka wystąpienia niezgodności lub częściowej niezgodności w przyszłości

Audyt zgodności z RODO - korzyści

Czas na krótkie podsumowanie, a najlepiej chyba w tej sytuacji wskazać jakie mogą płynąć korzyści z przeprowadzenia audytu zgodności z RODO.

- inwentaryzacja procesów przetwarzania danych,
- inwentaryzacja celów, zakresów przetwarzania danych, skali dostępu podmiotów trzecich, systemów informatycznych i innych istotnych składników procesów przetwarzania danych,
- ustalenie niezgodności (kryterium: zgodność z RODO i przepisami branżowymi w zakresie ochrony danych osobowych),
- rekomendacje w zakresie osiągnięcia zgodności z przepisami,
- punkt wyjścia do niektórych elementów wdrożenia – np. identyfikacja zagrożeń, które zostaną wykorzystane przy dokonywaniu oceny ryzyka, określenie właścicieli biznesowych poszczególnych procesów i przypisanie im obowiązków w zakresie ochrony danych osobowych, lista dokumentów i procedur do stworzenia / poprawienia.

Jeśli to wszystko co opisałem powyżej brzmi dla Ciebie skomplikowanie, nie załamuj rąk – jako iSecure możemy zrobić to za Ciebie ☺

Michał Sztąberek – ekspert w zakresie ochrony danych osobowych, prezes zarządu iSecure Sp. z o.o.