Warszawa, dn. 29.09.2026 r.

Jak wygląda proces audytu ochrony danych – od przygotowania po raport końcowy

Wstęp

Na wstępie klasycznie warto sobie wyjaśnić czym jest audyt ochrony danych. A zatem - audyt to usystematyzowany proces weryfikacji procesów przetwarzania danych osobowych oraz stosowanych zabezpieczeń pod kątem zgodności z przepisami prawa, a także dobrymi praktykami związanymi z RODO np. wynikającymi z norm ISO, itp.

Audyt powinien mieć dość jasną i klarowną strukturę. W naszym przypadku wygląda to następująco:

- Spotkanie otwierające i ustalenie harmonogramu prac.
- Zebranie wstępnych informacji i dokumentacji (kwestionariusze/ankiety wstępne).
- Wywiady z właścicielami procesów przetwarzania danych osobowych oraz szefem / pracownikami odpowiadającymi za IT.
- Ewentualne uzupełnienie dokumentacji niezbędnej do dokończenia analizy stanu faktycznego (jako następstwo wywiadów, ponieważ w ich trakcie może okazać się, że w firmie istnieją jeszcze jakieś inne / dodatkowe instrukcje / protokoły / praktyki w formie pisemnej, które nie zostały udostępnione audytorowi na wcześniejszym etapie – patrz: pkt drugi powyżej)
- Opracowanie raportu z audytu (w naszym przypadku: ogólnego dla najwyższego kierownictwa oraz szczegółowego będącego w zasadzie czymś na kształt *action planu*).
- Spotkanie zamykające i rekomendacje dalszych działań.

Najważniejsza kwestia - audyt nie jest kontrolą mającą na celu znalezienie winnych, lecz partnerską współpracą mającą na celu osiągnięcie zgodności z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych.

Spotkanie otwierające audyt

Wbrew pozorom to jeden z kluczowych momentów, bo daje szanse wzajemnego poznania się, ustalenia konkretnych zasad i reguł postępowania, udzielenie odpowiedzi na nurtujące pytania, itd.

Kto bierze udział w takim spotkaniu? Po stronie audytora będą to: reprezentant zarządu, audytor wiodący, audytor IT oraz dedykowany Inspektor Ochrony Danych (IOD). Po stronie klienta zaś: kadra menadżerska / zarząd oraz wyznaczony koordynator projektu.

Bardzo ważnym elementem spotkania otwarcia jest ustalenie albo potwierdzenie harmonogramu audytu. To właśnie w nim znajdziemy m.in. ustalone terminy przekazania ankiet wstępnych i listy dokumentów, ramy czasowe na zebranie dokumentacji przez klienta, a także planowane ramy czasowe spotkań audytowych oraz termin dostarczenia i omówienia raportu.

Kwestionariusze audytowe (ankiety wstępne i weryfikacja dokumentacji)

W moim przekonaniu, żeby sprawnie przeprowadzić audyt niezbędne jest sięgnięcie po ankiety wstępne (kwestionariusze audytowe). Dlaczego? Odpowiedź jest niezwykle prosta – dzięki nim możemy jako audytorzy dokonać pierwszego, wstępnego zmapowanie procesów przetwarzania danych, a także systemów informatycznych i obowiązujących w firmie procedur. To doskonała baza wiedzy dla audytorów przed przystąpieniem do kolejnego etapu, czyli wywiadów bezpośrednich.

Warto też wspomnieć jakie dokumenty i informacje są zbierane przez audytora. Będą to w szczególności: obowiązujące polityki i procedury RODO / bezpieczeństwa danych, klauzule informacyjne, umowy powierzenia, itd.

Wywiady audytowe (badanie procesów w praktyce)

Po skompletowaniu wypełnionych kwestionariuszy audytowych oraz dokumentacji udostępnionej przez audytowaną firmę można przystąpić do kolejnego etapu, czyli wywiadów bezpośrednich z właścicielami biznesowymi poszczególnych procesów przetwarzania danych osobowych.

Z kim i jak rozmawiają audytorzy? Jak zostało wspomniane powyżej – audytor będzie teraz prowadził indywidualne spotkania z kluczowymi właścicielami biznesowymi odpowiedzialnymi za miejsca, gdzie przetwarzane są dane osobowe. Poniżej lista takich przykładowych działów, które wymagają sprawdzenia:

- Kadry i Płace (HR),
- Marketing,
- Sprzedaż,
- Obsługa klienta,
- Księgowość,
- IT/Bezpieczeństwo IT,
- Administracja,
- Dział Prawny.

Ważne, by obie strony zarezerwowały sobie odpowiednią ilość czasu - zwykle od 40 minut do 1,5–2 godzin na obszar. Pamiętajmy, że rzetelnego audytu nie da się zrobić w pośpiechu.

Rozmowy audytowe mają charakter poznawczy i weryfikacyjny (audytor IT weryfikuje techniczne środki bezpieczeństwa, audytor wiodący weryfikuje procesy i formalności).

Po wywiadach jest jeszcze czas na dodatkowe pytania, uzupełnienie brakujących dokumentów i upewnienie się, że zebrany materiał jest kompletny.

Raport z audytu (analiza i opracowanie wyników)

Po zakończeniu wszystkich opisanych wcześniej etapów następuje praca analityczna audytorów. Łączone są ustalenia z wywiadów, dokumentów oraz audytu obszaru IT i tworzony jest na tej podstawie raport poaudytowy.

W naszej firmie przygotowujemy dwa raporty. Raport ogólny (*executive summary*), który skierowany jest do zarządu i kadry zarządzającej. Ten raport prezentuje najważniejsze niezgodności, ocenę ogólnego poziomu ryzyka oraz kluczowe rekomendacje strategiczne. Z kolei raport szczegółowy (np. w formie matrycy ryzyk i zaleceń) skierowany jest do właścicieli biznesowych, działu IT i koordynatorów. Zawiera szczegółowy wykaz luk, uchybień formalnych i technicznych oraz konkretne wytyczne dotyczące działań naprawczych krok po kroku.

Spotkanie zamykające audyt

Samo przygotowanie raportu to jednak za mało. Istotne jest, by jego kluczowe ustalenia zostały przekazane w zwięzły sposób kadrze zarządzającej i menadżerskiej. W tym celu organizowane jest spotkanie zamknięcia. W jego trakcie następuje omówienie wyników raportu „na żywo", wyjaśnienie wątpliwości i priorytetyzacja zaleceń.

Jeśli chodzi o uczestników takiego spotkania to wygląda to następująco. Po stronie audytora będzie to jego zespół (audytor wiodący, audytor IT, IOD, członek zarządu), natomiast po stronie audytowanej będą to kluczowi decydenci.

Przykładowa agenda spotkania:

- Przedstawienie głównych wniosków i skali zidentyfikowanych ryzyk.
- Omówienie planu naprawczego (*roadmapy wdrożeniowej*) – które luki należy zaadresować w pierwszej kolejności.
- Formalne zamknięcie etapu audytowego.

Podsumowanie

Audyt RODO to nie cel sam w sobie, lecz punkt wyjścia do budowy realnego, dopasowanego do organizacji systemu ochrony danych. Najważniejszą korzyścią biznesową będzie tu zminimalizowanie ryzyka kar i incydentów bezpieczeństwa, uporządkowanie wewnętrznych procesów, wzrost zaufania klientów i partnerów biznesowych.

Michał Sztąberek – ekspert ds. ochrony danych osobowych, CEO w iSecure Sp. z o.o.