Główne cele audytu ochrony danych

Z powodu coraz częstszych strat finansowych, jak i w szczególności wizerunkowych, działanie w zgodności z RODO i szeroko pojętą ochroną danych osobowych nie jest już traktowane tylko jako niepotrzebny obowiązek, lecz także jako działanie marketingowe, bardzo pożądane wśród kontrahentów lub klientów przedsiębiorstwa. Oprócz wdrażania rozwiązań zgodnych z RODO, przedsiębiorcy coraz częściej starają się posiadać i przedstawiać bezpośrednie dowody realizacji obowiązków. Jest to zjawisko występujące w szczególności w obszarach szeroko pojętych usług, w których przedsiębiorstwa działają głównie jako podmioty przetwarzające (procesorzy). Ze względu na małą obecnie ilość możliwych metod certyfikacji, najczęściej w celu udowodnienia zgodności z RODO przedsiębiorcy korzystają z usług zewnętrznych firm audytorskich, których celem jest przeprowadzenie kontroli zgodności i poświadczenie zgodności procesów przetwarzania z unijnymi i krajowymi przepisami dotyczącymi ochrony danych lub wskazanie braków. W takich sytuacjach często pojawia się zderzenie dwóch celów – przedsiębiorcy - przejawiające się w woli polepszenia swojego wizerunku, uzyskania korzyści jak i ograniczenia kosztów oraz celów audytorów - przejawiających się w woli przeprowadzenia jak najdokładniejszej kontroli celem wykrycia wszelkich nieprawidłowości. Czy niniejsze cele mogą ze sobą współistnieć?

NA CZYM POLEGA AUDYT?

Audyt zgodności z RODO jest wielopłaszczyznowy, może dotyczyć całego przedsiębiorstwa (ochrona wszystkich danych firmy) lub tylko wybranych procesów związanych z przetwarzaniem danych osobowych (np. ochrona danych pracowników w procesie “onboardingu” lub profilowanie danych w celach marketingowych). Najbardziej istotnym celem audytu jest sprawdzenie, czy całokształt działań przedsiębiorstwa lub konkretny proces jest dokonywany w sposób zgodny z tzw. zasadami ochrony danych określonymi w art 5 RODO. Niniejszą zgodność doświadczeni audytorzy weryfikują poprzez:

- mapowanie transferów danych (“śledzenie” losów danych osobowych od chwili ich zebrania aż do etapu końcowego np. archiwizacji lub usunięcia);
- analizowanie bazy danych (jak duża jest baza, jakie są podstawy prawne przetwarzania danych, jakie są cele wykorzystywania danych);
- inspekcje dokumentacji za pomocą której dochodzi do zbierania danych osobowych - nie tylko obecnej lecz także starej, zarchiwizowanej dokumentacji, gdzie najczęściej znajdują się nieprawidłowości.

Oprócz analizy przedstawionego materiału, audytorzy przeprowadzają rozmowy z kadrą kierowniczą i pracownikami przedsiębiorstwa, celem pozyskania jak największej informacji o sposobie działania przedsiębiorstwa, a w szczególności w celu zderzenia procedur obowiązujących w spółce z ich faktycznym stosowaniem i przestrzeganiem.

Specjalista dokonujący audytu w swej pracy nie może opierać się tylko na przepisach prawa w celu prawidłowego oszacowania ryzyka. Audyt obejmuje także praktyczne kwestie bezpieczeństwa, w szczególności sposoby zabezpieczenia danych przechowywanych w formie papierowej, jak i zabezpieczenia informatyczne np. stosowanie haseł, szyfrowanie korespondencji wychodzącej, firewalle, programy antywirusowe etc. W niektórych przypadkach audyt może być połączony z przeprowadzeniem testów penetracyjnych systemów IT lub może polegać na przeprowadzeniu

kontrolowanej prowokacji, mającej na celu sprawdzenie świadomości pracowników o istniejących procedurach lub działaniach pracowników pod wpływem stresu. Zwieńczeniem pracy audytora jest sporządzenie raportu, opisującego wszystkie wykryte ryzyka dla danych osobowych i naruszenia, przy jednoczesnym wskazaniu istotności danego ryzyka (zależnie od przyjętej metodologii sposoby opisania istotności mogą być różne), połączonym ze wskazaniem zaleceń dotyczących sposobu wprowadzenia stanu pożądanego. Bardzo często umowa z zewnętrzną firmą na realizację audytu jest połączona z objęciem funkcji zewnętrznego inspektora ochrony danych. Z powyższych powodów audyt może być traktowany jako mapa zadań, która będzie realizowana po zakończeniu audytu wraz z audytorem obejmującym funkcję inspektora ochrony danych osobowych.

KIM JEST AUDYTOR?

Audytor ochrony danych osobowych jest osobą posiadającą szeroką wiedzę i bogate doświadczenie z zakresu ochrony danych osobowych. Cechą bardzo pożądaną u audytora jest także znajomość branży audytowanej spółki, jego wiedza obejmuje nie tylko kwestie prawne, ale również kwestie praktyczne ochrony danych osobowych. Do najistotniejszych cech audytora należy jego bezstronność. Audytor nie ocenia klienta, nie opiera swojej decyzji na emocjach. Zastrzeżenia audytora dotyczą tylko kwestii ochrony danych osobowych i zgodności procesów z wymogami prawnymi. Audytorzy co do zasady są zobowiązani do zachowania poufności, ponadto w celu uniknięcia potencjalnych naruszeń i wprowadzania u klientów dyskomfortu, audytorzy bardzo często ograniczają zakres danych przesyłanych drogą elektroniczną lub papierową, dokonując inspekcji na miejscu w siedzibie lub placówce klienta. Audytor nie sugeruje odpowiedzi, pozwalając osobie audytowanej na swobodną wypowiedź. Dzięki praktyce zawodowej, dokładnie wie, które obszary należy z większą dokładnością i precyzją sprawdzić, a także w jaki sposób należy sformułować pytanie by uzyskać najpełniejszą wypowiedź. Audytor zawsze stara dopasować się do możliwości klienta. Ustalenie terminów spotkań, czytania dokumentacji jak i rozmów z pracownikami są podejmowane tylko za zgodą i wiedzą przedsiębiorstwa.

PUŁAPKI AUDYTU

Przedsiębiorcy bardzo często w celu uzyskania jak najkorzystniejszego raportu i możliwości stosowania go jako dowodu przed kontrahentami, unikają odpowiadania na kłopotliwe zagadnienia lub nie przekazują Audytorom informacji i dokumentów, które mogą stawiać spółkę w złym świetle. Audytor nie jest organem państwowym przeprowadzającym kontrolę - audytor nie działa na szkodę Klienta. Kontrola natomiast dotyczy tylko informacji przekazanych bezpośrednio przez klienta lub pozyskanych w toku obserwacji np. oględzin miejsc przetwarzania danych osobowych wraz z osobą wyznaczoną przez spółkę. Utrudnianie audytorowi przeprowadzenia audytu jest działaniem kontrproduktywnym, działającym na własną szkodę. Celem audytora nie jest “ukaranie” przedsiębiorcy tylko udzielenie pomocy w jak największym możliwym stopniu. Nieprzekazanie audytorowi informacji o potencjalnych ryzykach nie skutkuje ich zniknięciem ani wygaszeniem. Przedsiębiorcy bardzo często nie posiadają świadomości o potencjalnych nieprawidłowościach, a także o ich potencjalnych skutkach. W odróżnieniu od możliwego wycieku danych, przekazanie informacji audytorom nie skutkuje problemami wizerunkowymi dla przedsiębiorcy, gdyż audytorzy są zobowiązani do zachowania poufności. Udzielenie pełnych informacji zgodnych ze stanem faktycznym jest tym bardziej istotne, jeżeli przeprowadzenie audytu jest związane z przejęciem funkcji inspektora ochrony danych. Inspektor ochrony danych osobowych, który nie dysponuje pełną wiedzą o procesach przetwarzania nie może w sposób prawidłowy pełnić swej funkcji. Przykładowo. w przypadku braku wiedzy o transferze danych poza EOG, nie jest w stanie wydać prawidłowej opinii odnośnie zawarcia umowy

powierzenia, poinformowania podmiotów danych osobowych o przetwarzaniu danych lub znalezieniu podstawy prawnej takiego transferu, co może skutkować znacznymi kosztami dla przedsiębiorcy. Utrudnianie zatrudnionemu audytorowi przeprowadzenie audytu jest działaniem stricte na niekorzyść przedsiębiorstwa i utrudnia lub uniemożliwia wykonanie celu, w jakim zawarta została umowa z firmą audytorską.

Oprócz unikania kwestii problematycznych, częstym problemem występującym podczas audytu jest także zbytnia pasywność personelu przedsiębiorstwa - zbyt lakoniczne wypowiedzi lub stosowanie zbyt ogólnych, bezpiecznych odpowiedzi na zadane sformułowania, nie pozwalające audytorowi na pełne zrozumienie wewnętrznych procesów spółki. Rozmowa z audytorem nie powinna stanowić tylko obowiązku, lecz także stanowić szansę na poszerzenie swojej wiedzy z zakresu bezpieczeństwa danych osobowych. Pełna współpraca z audytorem nie tylko pozwala na sporządzenie pełniejszego raportu, lecz także na jego szybsze zakończenie.

EFEKTY AUDYTU

Audyty są bardzo przydatnym procesem dla przedsiębiorstwa - nie tylko na gruncie ochrony danych osobowych, lecz także innych obszarów. Najistotniejsze jest by w czasie jego przeprowadzania, nie zgubić celu, dla którego zostaje przeprowadzony. Jego zamiarem jest wykrycie i usunięcie nieścisłości w celu osiągnięcia jak największej efektywności i bezpieczeństwa dla spółki, nie zaś jako reklama sama w sobie. Reklamą będzie stabilność, renoma, a w szczególności komfort bezpieczeństwa, który uzyskają klienci lub kontrahenci.