Warszawa, dn. 05.04.2023 r.

Dziewięć najważniejszych obszarów, które powinieneś uwzględnić w swojej polityce ochrony danych osobowych

Wydaje się, że polityka ochrony danych osobowych (dalej jako PODO) to podstawowy dokument opisujący zasady obowiązujące w organizacji w interesującym nas temacie, czyli… ochronie danych osobowych. PODO można napisać w bardzo różny sposób. Można z tego zrobić dość obszerny i szczegółowy dokument albo pójść w kierunku czegoś nieco bardziej ogólnego, ale odsyłającego do bardziej rozbudowanych i zawierających konkretne obowiązki, nakazy, zakazy, itp. załączników.
Osobiście preferuję ten drugi model przygotowywania PODO i to właśnie na nim skupię się w poniższym artykule.

(1) Cel i zakres

To taka niby oczywista-oczywistość, cytując klasyka. W każdym razie określenie celu i zakresu danej procedury / dokumentu to absolutna podstawa. W przypadku PODO nadrzędnym celem jest chęć uregulowania – w jednym bądź kilku dokumentach – wszystkich obszarów, które odnoszą się do procesów przetwarzania danych oraz przyjętych w organizacji środków technicznych i organizacyjnych. Oczywiście można to jeszcze bardziej rozbudować, ale tak jak wspomniałem powyżej – to jest cel zasadniczy istnienia PODO. A zakres? No cóż, dane osobowe…

(2) Odpowiedzialność

Jak nie przypiszesz odpowiedzialności za dokument nie licz na to, że ktokolwiek będzie poczuwał się do przygotowywania jakichkolwiek jego aktualizacji, przeglądów, itd. A przecież na każdym szkoleniu krzyczą: wdrożenie RODO to proces, a nie jednorazowa czynność. A zatem jeśli nikogo nie przypiszesz do odpowiedzialności za PODO, to jesteś na doskonałej drodze do popełnienia tego klasycznego błędu – potraktujesz wdrożenie wymogów wynikających z unijnego rozporządzenia jako jednorazowy zryw zgodności ;-)

(3) Najważniejsze terminy pojawiające się w PODO

Tak, chodzi o najbardziej klasyczny słowniczek pojęć, które pojawią się – i tu uwaga – tak w PODO jak i ew. załącznikach do polityki. Dzięki temu wszystko będzie w dokumencie otwierającym, stanowiącym niejako przewodnik po istniejącym w Twojej organizacji systemie ochrony danych osobowych. Taki wykaz terminów najlepiej przygotować na końcu jak już będziesz miał pełen obraz jakimi pojęciami posługiwałeś się w poszczególnych dokumentach. Tylko zapisuj je sobie na etapie przygotowywania procedur, żebyś o czymś nie zapomniał.

(4) Deklaracja stosowania

Zgadłeś, tę część pożyczyłem z metodologii opisanej choćby w normie ISO 27001. Ale to naprawdę wartościowa część PODO, bo jest to miejsce, gdzie zarząd może jasno wskazać jak

bardzo ważna jest dla niego kwestia ochrony danych osobowych. Przykład idzie z góry, a zatem sam już rozumiesz, dlaczego ta część PODO powinna się pojawić w Twoim dokumencie.

(5) Czynniki zewnętrzne i wewnętrzne istotne dla celu działania organizacji

I znowu sięgamy po normę ISO 27001. Ale, ale – tu musisz się trochę napracować i wysilić. Przykładowym czynnikiem zewnętrznym może być pozycja rynkowa Twojej firmy, powszechnie obowiązujące prawo, itp. Przykładowym czynnikiem wewnętrznym z kolei będzie np. struktura organizacyjna, a także wewnętrzne regulacje i procedury obowiązujące w organizacji.

(6) Role i odpowiedzialność za bezpieczeństwo danych osobowych

Jak sama nazwa wskazuje, to przestrzeń, w której opisujemy głównych aktorów występujących na deskach naszego teatru, a zatem zarząd (jako reprezentant administratora), IOD (wiadomo), specjaliści IT (kwestie związane z bezpieczeństwem danych od strony technicznej), itd. Nie zapomnij o właścicielach biznesowych (tak, na nich spoczywać będzie naprawdę sporo zadań. Pamiętasz? Przykład idzie z góry) i zwykłych użytkownikach, czyli osobach, które na co dzień pracują na danych osobowych.
Dobra, podam Ci teraz parę przykładów zadań poszczególnych aktorów:

- zarząd: zatwierdzanie i publikowanie dokumentów i procedur związanych z ochroną danych osobowych dotyczących wszystkich pracowników i współpracowników Spółki;
- IOD: zadania wprost opisane w RODO;
- właściciele biznesowi: identyfikowanie podatności i zagrożeń dla nadzorowanych procesów przetwarzania danych i przekazywanie w tym zakresie informacji do właściwych osób (np. IOD) i jednostek organizacyjnych (np. dział IT);
- pracownicy IT: dbanie o poprawne i efektywne działanie administrowanych systemów teleinformatycznych;
- użytkownicy: zapewnienie poufności w stosunku do wszystkich danych osobowych przetwarzanych w organizacji.

(7) Szkolenia i edukacja

Masz PODO, ale nikt jej nie stosuje? Bez działań edukacyjnych i ciągłego „trąbienia" o ochronie danych osobowych nawet najlepsze procedury i środki techniczne nie dadzą rady. Dlatego już w polityce warto poświęcić temu obszarowi stosowny fragment i wskazać, że jest to istotny element determinujący to jak w Twojej organizacji postrzega się temat ochrony danych osobowych.

(8) Audyt

Wdrożyłeś RODO w 2018 r. i jesteś z siebie dumny? Wierzę, że wykonałeś wtedy dużą robotę, ale mam też złą wiadomość. Mamy rok 2023, Twój system ochrony danych mógł najnormalniej w świecie mocno się zdezaktualizować. Zobacz, ile w tzw. międzyczasie pojawiło się decyzji PUODO, zerknij na opinie EROD, itd. Jest tego całe mnóstwo. Bez regularnych audytów tak zgodność z przepisami o ochronie danych jaki i ich bezpieczeństwo

są mocno zagrożone. Dlatego audyt to podstawa. I to regularny audyt. Zapisz to w PODO i pilnuj, by był wykonywany.

(9) Przegląd i aktualizacja PODO

Ta część to w sumie naturalna konsekwencja tego, że traktujesz ochronę danych osobowych jako proces a nie jednorazowy zryw, bo komuś przypomniało się o RODO. Świat ruszył do przodu od 2018 r., miałeś pewnie już różne doświadczenia z naruszeniami, widziałeś co punktuje w swoich decyzjach organ nadzorczy, regularnie robisz audyty i pracujesz nad usuwaniem niezgodności. Doskonale, uwzględnij to zatem w PODO. Wskaż częstotliwość przeglądów, osobę za to odpowiedzialną, itd.

No dobrze, a gdzie te wszystkie szczegółowe procedury jak np. obsługa incydentów ochrony danych, realizowania praw podmiotów danych, itd. Tak jak napisałem na wstępie, w swojej praktyce preferuję PODO opisującą to co wskazałem powyżej, a przysłowiowe „mięsko" trafia do bardziej szczegółowych instrukcji i procedur. Przy czym istotne jest to, że już w PODO do nich odsyłam poprzez ich wymienienie wraz z krótką informacją czego dotyczą. Dzięki temu dzielisz dokumentację ochrony danych osobowych na bardziej „zjadliwe" części i – mówiąc już zupełnie żartobliwie – nie zabijesz nikogo ilością stron, przez które będzie się trzeba przekopać…

Michał Sztąberek – prezes zarządu w iSecure Sp. z o.o.