Warszawa, 21.10.2020

Dokumentacja zgodna z RODO

“Proszę o sporządzenie dokumentacji wewnętrznej zgodnej z RODO” - jest to jedno z najczęściej pojawiających się próśb skierowanych przez przedsiębiorców do wewnętrznych inspektorów ochrony danych lub spółek zajmujących się doradztwem z zakresu ochrony danych osobowych. Poza pewnymi dokumentami będącymi nowością na gruncie RODO, np. rejestrem czynności przetwarzania lub dokumentami istniejącymi od dawna, jako obowiązkowe, a zmienionymi mocą rozporządzenia, np. umową powierzenia, RODO w sposób bardzo lakoniczny wskazuje, jak należy dostosować czynności przetwarzania danych do wymogów RODO, aby zostały uznane za zgodne z zasadą rozliczalności oraz organizacyjnie wystarczające do zabezpieczenia danych. Jakie zatem elementy powinna zawierać dokumentacja zgodna z RODO?

Polityka ochrony danych osobowych

Jest to najistotniejszy dokument potwierdzający, że przedsiębiorca posiada organizacyjne sposoby zabezpieczenia danych. Dokument może przybierać różne nazwy - bardzo często jest zwany “Polityką bezpieczeństwa informacji (PBI)” lub “Polityką ochrony danych osobowych (PODO)”. Głównymi elementami omawianej polityki są:

1. **Preambuła -** określająca:
    a. podmioty zobowiązane do jej przestrzegania;
    b. powody jej uchwalenia;
    c. zakres stosowania;
    d. podstawy prawne zobowiązujące do jej przestrzegania;
    e. słownik pojęć.

2. **Ustalenie zakresu obowiązków osób odpowiedzialnych za zapewnienie bezpieczeństwa danych osobowych.** Najczęściej pojawiającym się podziałem i zakresem kompetencji jest (wyliczenie ma charakter wyłącznie przykładowy i nie są to jedyne kompetencje):
    a. **Administrator danych osobowych** - reprezentowany przez właściciela spółki lub zarząd (albo jednoosobowo – przez Prezesa)
        - zapewnia niezależność działań IOD;
        - jest odpowiedzialny za podjęcie decyzji w zakresie zgłaszania naruszeń;
        - powołuje IOD;
        - zapewnia narzędzia techniczne i organizacyjne pozwalające na prawidłową realizację zadań przez IOD;
        - upoważnia do przetwarzania danych lub nadaje uprawnienia do nadawania w jego imieniu upoważnień (np. przez dział kadr).
    b. Inspektor ochrony danych (IOD)
        - informuje administratora danych osobowych o wykrytych nieprawidłowościach;
        - wspiera w prowadzeniu rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania;
        - reprezentuje administratora w kontaktach z organem nadzorczym lub przynajmniej stanowi pierwszą linię kontaktu;
        - bierze udział w prowadzeniu analizy ryzyka;

- pomaga prowadzić rejestr naruszeń oraz rejestr umów powierzenia;
- przeprowadza okresowe audyty
- informuje administratora danych o jego obowiązkach i doradza mu w tej sprawie.

c. **Administrator systemów informatycznych (ASI) - czasem zwany w sposób ogólny "działem IT":**
   - wspiera administratora danych i IOD w zakresie zapewnienia bezpieczeństwa systemów informatycznych;
   - bierze udział w analizie naruszeń ochrony danych osobowych;
   - weryfikuje i ewidencjonuje uprawnienia do systemów informatycznych;
   - uczestniczy w procesach analizy ryzyka.

d. **Właściciel biznesowy**
   - jest zobowiązany do weryfikowania przestrzegania postanowień polityki przez podwładnych;
   - kontaktuje się i wspiera IOD we wdrażaniu nowych procesów przetwarzania danych;
   - promuje bezpieczeństwo i świadomość ochrony danych.

e. **Pracownicy i współpracownicy (personel) / osoby upoważnione do przetwarzania danych**
   - przestrzegają postanowień polityki;
   - zgłaszają naruszenia;
   - są zobowiązani do zachowania poufności;
   - dbają o zabezpieczenie danych osobowych.

f. **Personel pomocniczy/personel nieupoważniony do przetwarzania danych**
   - zobowiązany do zachowania poufności;
   - zobowiązany do zapewnienia bezpieczeństwa w obszarze, w którym przebywa.

3. **Wskazanie zasad odpowiedzialności za naruszenie zapisów polityki**
4. **Wskazanie i opisanie procesów (czynności) przetwarzania danych osobowych (zalecane)**

Polityka ochrony danych osobowych swym zakresem powinna obejmować wszystkie procesy przetwarzania danych w ramach spółki. Mając na uwadze, jak wielki może to być zakres, odradza się tworzenie zbyt szczegółowego dokumentu - **głównym celem polityki jest stworzenie podstaw ochrony danych osobowych w ramach spółki**, które następnie powinny zostać doprecyzowane w innych dokumentach wewnętrznych, opisujących szczegółowo zagadnienia związane z wymogami ochrony danych. Stworzenie rozproszonego modelu zasad ochrony danych osobowych nie jest jednak wymagane. Bardzo częstym zjawiskiem jest tworzenie dużych polityk regulujących wszystkie zagadnienia związane z ochroną danych osobowych. Taka forma może być przytłaczająca dla pracowników i nieczytelna. Znacznie korzystniejszym rozwiązaniem jest umieszczenie w treści polityki odnośników do poszczególnych dokumentów wewnętrznych regulujących daną materię (np. odrębnych załączników, regulaminów, procedur).

Przedstawiona poniżej lista dokumentów i przykładowa zawartość, stanowi propozycję z naszej strony. Dotyczy ona dokumentów, które mogą być częścią polityki ochrony danych, jako np. integralne załączniki do niej lub obowiązywać jako odrębne dokumenty, powiązane z polityką ochrony danych. Możliwe jest oczywiście przyjęcie innego nazewnictwa, a także rozdrobnienie lub skonsolidowanie dokumentów. Jednakże powinny one dla realizacji zasady rozliczalności regulować wskazane zagadnienia.

Instrukcja zarządzania systemami informatycznymi (IZSI)

Dokument zwany także "polityką bezpieczeństwa systemów informatycznych (PBSI)" ma na celu uregulowanie zasad wykorzystywania systemów informatycznych w ramach spółki. Dokument najczęściej jest podzielony na dwie części. Jest to polityka, za której przegląd z zasady odpowiedzialny jest ASI (Dział IT), a za przestrzeganie - cały personel korzystający z systemów informatycznych.

1. **Obowiązki ASI (katalog wyłącznie przykładowy):**
    a. ustalenie i weryfikacja wymogów technicznych, jakie musi spełniać system informatyczny zanim będzie mógł być wykorzystywany do przetwarzania danych osobowych;
    b. opracowanie lub nadzorowanie zasad przeprowadzania backupów;
    c. zarządzanie nadawaniem/modyfikacją/odebraniem uprawnień do systemów informatycznych;
    d. przygotowanie wzoru wniosku o nadanie uprawnień;
    e. przestrzeganie zasad przechowywania kont administratora do systemów;
    f. zarządzanie polityką autoryzacji (np. haseł);
    g. przegląd praw i uprawnień użytkowników w systemach;
    h. zabezpieczenie sieci;
    i. realizowanie zasad konserwacji, naprawy i utylizacji sprzętu;
    j. uzgodnienie zasad monitoringu działań w systemach informatycznych (gdy ma zastosowanie);
    k. ustalenie zasad przechowywania metadanych aplikacji i nośników danych.

2. **Obowiązki pracownika (katalog wyłącznie przykładowy):**
    a. przestrzeganie zasad składania wniosków o nadanie uprawnienia, w tym:
        - kto inicjuje proces (kierownik czy pracownik);
        - kto nadaje uprawnienia (ASI czy inne osoby wskazane);
        - kto ewidencjonuje uprawnienia (ASI czy konkretna jednostka).
    b. przestrzeganie zasad wykorzystywania skrzynki pocztowej (ze wskazaniem tych zasad);
    c. przestrzeganie zasad wykorzystywania nośników informacji (ze wskazaniem tych zasad);
    d. przestrzeganie zasad działania w ramach pracy zdalnej (ze wskazaniem tych zasad);
    e. przestrzeganie zasad wykorzystania aplikacji (ze wskazaniem tych zasad);
    f. przestrzeganie zasad transferu danych (ze wskazaniem tych zasad);
    g. przestrzeganie zasad zabezpieczenia danych, pomieszczeń i nośników (ze wskazaniem tych zasad).

Procedura privacy by design and by default

Taka procedura jest jednym z najistotniejszych dokumentów związanych z realizacją zasady rozliczalności. Jak sama nazwa wskazuje, jej głównym celem jest realizacja zasady privacy by design and by default, czyli zapewnienia, że dane osobowe są przetwarzane zgodnie z wymogami rozporządzenia od chwili ich pozyskania, a także przez cały okres ich przetwarzania. Bardzo często w ramach takiej procedury, opisuje się sposoby realizacji związanych z powyższą zasadą obowiązków

ciążących na mocy RODO, związanych z prowadzeniem dokumentacji lub wdrażaniem nowych procesów w firmie.

1. **Zasady projektowania nowych procesów przetwarzania danych**
    a. opisanie, kto inicjuje proces kontaktu z IOD w celu zaopiniowania nowego procesu przetwarzania danych;
    b. przyjęcie oficjalnych wzorów, służących realizacji zasady rozliczalności, np. formularz audytowy zawierający:
        - zakres danych
        - kategorię podmiotów danych osobowych
        - cel przetwarzania
        - planowany okres retencji danych
        - opis planowanych odbiorców danych osobowych
    c. ustalenie, kto jest odpowiedzialny za podjęcie decyzji za wdrożenie procesu.
2. **Zasady analizy prawnie uzasadnionego interesu**
    a. opisanie, kto inicjuje proces kontaktu z IOD w celu przeprowadzenia analizy prawnie uzasadnionego interesu, jako podstawy prawnej przetwarzania danych;
    b. przyjęcie oficjalnych wzorów (np. dot. przeprowadzonej analizy, klauzuli informacyjnej), służących realizacji zasady rozliczalności;
    c. ustalenie, kto jest odpowiedzialny za podjęcie decyzji za wdrożenie procesu lub podjęcie działań naprawczych.
3. **Transfer danych osobowych**
    a. opisanie, kto inicjuje proces kontaktu z IOD w celu zaopiniowania transferu danych (w szczególności poza Europejski Obszar Gospodarczy);
    b. wskazanie, jakie działania należy podjąć w przypadku planu transferu danych poza spółkę;
    c. przyjęcie wzorca umowy powierzenia;
    d. ustalenie, kto jest odpowiedzialny za zawarcie umowy powierzenia;
    e. przyjęcie zasad weryfikacji podmiotów przetwarzających;
    f. przyjęcie wzorca formularza audytowego dla podmiotu przetwarzającego.
4. **Rejestr czynności przetwarzania (RCP)**
    a. wskazanie osób odpowiedzialnych za prowadzenie RCP;
    b. wskazanie wzoru RCP;
    c. wskazanie zasad przechowywania RCP;
    d. wskazanie roli IOD i właścicieli biznesowych, a także IT w procesie tworzenia RCP.
5. **Rejestr kategorii czynności przetwarzania (RKCP)**
    a. wskazanie osób odpowiedzialnych za prowadzenie RKCP;
    b. wskazanie wzoru RKCP;
    c. wskazanie zasad przechowywania RKCP;
    d. wskazanie roli IOD i właścicieli biznesowych, a także IT w procesie tworzenia RKCP.
6. **Zasady kontroli i audytu**
    a. określenie częstotliwości przeprowadzania audytów zgodności z zasadami ochrony danych osobowych w ramach spółki;
    b. przyjęcie terminów weryfikacji dokumentacji wewnętrznej;
    c. wskazanie osób odpowiedzialnych za przeprowadzenie audytów;
    d. przyjęcie oficjalnych wzorów dokumentacji audytowej lub raportu.

Procedura retencji danych osobowych

Do tej pory jest to jeden z najrzadziej występujących dokumentów w praktyce, jednocześnie będący równie istotnym dla udowodnienia realizacji zasady rozliczalności. Celem dokumentu jest opisanie okresów przechowywania danych osobowych. Mając na uwadze, że w ramach spółki, te same dane osobowe często są wykorzystywane w ramach różnych procesów, spółki w celu zachowania przejrzystości postanawiają znacząco rozszerzyć cel dokumentu poza ramy samego opisu retencji. Dokument zależnie od przyjętej szczegółowości, przybiera różne formy i może on opisywać:

1. **Kategorie dokumentacji**
    a. ściśle poufna;
    b. poufna;
    c. standardowa;
    d. publiczna.
2. **Podział danych osobowych na**
    a. rodzaje dokumentów (sądowa, kadrowa, ZFŚS);
    b. kategorie danych/osób (pracownicy, klienci, użytkownicy, subskrybenci);
    c. wskazanie nośnika/formy przetwarzania danych (elektronicznie, papierowo, w aplikacji, z wykorzystaniem cookies).
3. **Okresy retencji danych osobowych (element konieczny)**
    a. ścisłe - 2 lata od zakończenia sprawy, rok od uzyskania;
    b. luźne - do czasu wyrażenia sprzeciwu, do czasu posiadania konta w serwisie.
4. **Zasady dostępu (zalecane)**
    a. dostęp dla określonej jednostki - kadry, dział compliance;
    b. wskazanie osób nieupoważnionych - osoby bez upoważnienia, osoby niezwiązane ze spółką.

Powyższy wykaz dokumentów i ich zalecane elementy to jedynie przykłady, jakie treści mogą się znaleźć w polityce ochrony danych. Warto w swojej firmie sprawdzić, czy istnieją również niżej wymienione dokumenty, które również mogą wchodzić w skład takiej polityki (wykaz przykładowy):

1. procedura nadawania upoważnień
2. procedura reagowania na incydenty
3. zasady nadawania upoważnień
4. zasady dostępu do serwerowni
5. polityka dysponowania kluczami dostępu do pomieszczeń
6. polityka monitoringu wizyjnego

Ostatecznie, to firma określa, które dokumenty są jej niezbędne do wdrożenia, aby prawidłowo wykazać, że wprowadziła właściwe, dobrane do ryzyka, środki organizacyjne służące nie tylko prawidłowemu zabezpieczeniu danych, ale też wykazaniu spełnienia obowiązków, o których mowa w RODO.

Damian Bielecki, Specjalista ds. Ochrony danych osobowych w iSecure Sp. z o.o.