Warszawa, 18.10.2023 r.

Jak (nie) pisać polityki prywatności – dobre praktyki

„Polityka prywatności" - dokument umieszczany na witrynie internetowej w celu poinformowania użytkowników o tym, jakie dane osobowe są o nich zbierane i jak będą wykorzystywane.[1]

Wstęp

Wydawać by się mogło, że temat polityki prywatności został już omówiony wzdłuż i wszerz – wszystko co mogło zostać powiedziane, zostało powiedziane. Mainstream ochrony danych osobowych przepełniony jest publikacjami, poradnikami, artykułami, manualami czy wytycznymi dotyczącymi tego co, gdzie i jak należy ująć w treści polityki prywatności.

Stąd nie do końca zrozumiałe jest, dlaczego wciąż na rynku obserwujemy tak różne, w przeważającej mierze, błędne podejście do tematu. To co wysuwa się na pierwszy plan to chaos informacyjny lub treściowy – polityki prywatności składają się ze ściany tekstu, przez który, niczego winny użytkownik musi się „przekopać" żeby znaleźć informacje, które go dotyczą i interesują. Zadanie jest dodatkowo utrudnione, jeżeli informacje na zbieżny temat są porozsiewane po całym dokumencie a użytkownik próbuje złożyć je w całość niczym pojazd z Lego Technics.

Sukcesem jest, jeżeli polityka prywatności, pomimo wspomnianego chaosu zawiera wszelkie niezbędne, wyczerpujące i prawidłowe informacje dotyczące przetwarzania danych osobowych użytkowników strony internetowej – ale w praktyce tak nie jest. Być może wynika to właśnie z chaosu, ponieważ sam autor nie jest w stanie ogarnąć co, gdzie i w jaki sposób ujął lub należy jeszcze ująć, chociaż moim zdaniem to brak elementarnej wiedzy w zakresie ochrony danych osobowych.

Tworząc politykę prywatności należy przede wszystkim sięgnąć do przepisów prawa (RODO) w zakresie obowiązków nałożonych na administratora związanych ze spełnieniem obowiązku informacyjnego względem użytkownika (podmiotu danych), oraz zasad przetwarzania danych osobowych i ich praktycznej realizacji (głównie zasady rzetelności i przejrzystości).

W dalszej części artykułu skupię się na analizie i wskazaniu dobrych praktyk, ale wychodząc od najczęściej spotykanych błędów przy konstruowaniu polityk prywatności.

PROBLEM I

Bezrefleksyjne kopiowanie, „inspirowanie" rozwiązaniami innych podmiotów z rynku.

„*W sumie to oni robią dokładnie to co my*", „*Ich strona jest praktycznie taka sama*", „*Weźmy od nich i dostosujmy do nas*" – pomijając kwestie praw autorskich, analizując strony internetowe, już na pierwszy rzut oka widać, czy takie stwierdzenia pojawiały się przy okazji opracowania polityki prywatności. Jeżeli zbyt mocno polegamy na „inspiracji" i nie filtrujemy informacji w nich zawartych to w efekcie opracowana polityka prywatności nie odwzoruje faktycznych procesów przetwarzania danych osobowych na naszej stronie internetowej.

Treść polityki prywatności musi odwzorowywać faktyczne procesy przetwarzania danych osobowych. Procesy przetwarzania danych osobowych to, co do zasady, nic innego jak poszczególne funkcjonalności strony internetowej np.: formularze kontaktowe, oceny satysfakcji klientów, rejestracja/zgłoszenie reklamacji albo zwrotu. W polityce prywatności wymagane jest, aby znajdowały się informacje odpowiadające przetwarzaniu danych osobowych w poszczególnych procesach (funkcjonalnościach).

[1] źródło: https://pl.wikipedia.org/wiki/Polityka_prywatno%C5%9Bci

Jeżeli powyższa tożsamość nie jest zachowana, powstaje ryzyko, że użytkownik otrzymuje błędne informacje dotyczące przetwarzania danych osobowych albo nie otrzymuje ich w ogóle – co stanowi naruszenie przepisów ochrony danych osobowych tj. art. 13 lub 14 RODO. Naruszenie przepisów naraża administratora na odpowiedzialność, w szczególności kary administracyjne w wyniku postępowania przed Prezesem Urzędu Ochrony Danych Osobowych („PUODO").

PROBLEM II

Polityka prywatności nie zawiera wszystkich informacji na podstawie art. 13 lub 14 RODO.
Dlaczego polityka prywatności ma zawierać informacje na podstawie art. 13 lub 14 RODO? – bo polityka prywatności to nic innego jak obowiązek informacyjny.
Warto w tym miejscu przypomnieć co na gruncie RODO musi zawierać obowiązek informacyjny, komunikowany podmiotowi danych w kontekście polityki prywatności.
Zgodnie z art. 13 RODO:

- ✓ informacja o administratorze danych tj. dane rejestrowe;
- ✓ wskazanie czy u administratora został powołany Inspektor Ochrony Danych Osobowych („IOD");
- ✓ dane kontaktowe administratora / IOD;
- ✓ cele oraz podstawy przetwarzania danych
- ✓ odbiorcy danych (podmioty trzecie którym przekazywane są dane lub ich kategorie);
- ✓ informacja czy występują transfery danych poza EOG a jeżeli tak, to jaka jest postawa legalizująca;
- ✓ okresy retencji danych
- ✓ opisanie praw podmiotu danych, w tym prawa do wniesienia skargi oraz jak to zrobić;
- ✓ wskazanie czy podanie danych jest wymogiem umownym czy ustawowym i jakie są konsekwencje ich niepodania;
- ✓ informacja o zautomatyzowanym przetwarzaniu w tym profilowaniu;
- ✓ jeżeli przetwarzanie odbywa się na podstawie zgody to informacja o prawie do jej cofnięcia i jak to zrobić;

dodatkowo, jeżeli dane nie pochodzą bezpośrednio od podmiotu danych (użytkownika), zgodnie z art. 14 RODO:

- ✓ wskazanie w jaki sposób dane osobowe zostały pozyskane i od kogo;
- ✓ kategorii danych osobowych jakie zostały pozyskane i są przetwarzane przez administratora.

Prawidłowo opracowana polityka prywatności musi zawierać wszystkie powyższe informacje. Niezrozumiałą tendencją jest pomijanie niektórych z wyżej wymienionych elementów w treści polityki prywatności tj. m. in. informacji o transferach lub informacji o zautomatyzowanym przetwarzaniu w tym profilowaniu (najczęściej „niespotykane"). Na nasze pytanie, dlaczego te elementy są tak często pomijane, otrzymujemy odpowiedź „*bo ich nie ma*", „*nie występują*" – bardzo duży błąd!! Skoro jest wymóg ustawowy (art. 13, 14 RODO) to należy wskazać, że nie występują. Nie można antycypować wiedzy i świadomości podmiotu danych (użytkownika strony internetowej) w tym względzie.
Niewskazanie w treści polityki prywatności wszystkich wymaganych elementów na gruncie art. 13 lub 14 RODO, stanowi naruszenie ochrony danych osobowych, opisane powyżej w ostatnim akapicie PROBLEMU I.

PROBLEM III

Brak wydzielenia w polityce prywatności poszczególnych procesów przetwarzania danych (funkcjonalności strony internetowej).
Przeważająca ilość polityk prywatności z jakimi stykamy się na co dzień ma formę jednej, obszernej, skomplikowanej, przez co nieczytelnej i niezrozumiałej klauzuli informacyjnej. Praktyka rynkowa

pokazuje, że jeżeli nawet zachowane są wszystkie elementy wymagane na podstawie art. 13 lub 14 RODO (obowiązek informacyjny) to prezentowane są zbiorczo w jednym miejscu. Tytułem przykładu: przedstawienie celów i podstaw przetwarzania łącznie dla wszystkich procesów przetwarzania danych osobowych na stronie internetowej (funkcjonalności), bez wyraźnego oddzielenia. Takie ujęcie może powodować, że użytkownik, niemający wiedzy merytorycznej w zakresie ochrony danych osobowych, nie będzie w stanie jednoznacznie określić które cele i podstawy przetwarzania związane są np.: z przetwarzaniem jego danych osobowych dla skorzystania z formularza kontaktowego. Ktoś powie – można to „właściwie" opisać, tak – tworząc przy tym ścianę tekstu, na czym cierpi zasada przejrzystości (jedna z podstawowych zasad określona w art. 5 ust. 1 lit. a) RODO). Nie należy zapominać, że informacje dla podmiotu danych mają być komunikowane w prosty, jasny i zrozumiały dla niego sposób, w szczególności tyczy się to obowiązku informacyjnego. Niezgodność z podstawowymi zasadami przetwarzania danych osobowych również powoduje naruszenie ochrony danych osobowych na gruncie RODO.
Jak właściwie przekazać wszystkie informacje związane z przetwarzaniem danych osobowych w poszczególnych procesach przetwarzania (funkcjonalnościach) za pośrednictwem strony internetowej??

POLITYKA PRYWATNOŚCI = KLAUZULE INFORMACYJNE

Podejście do prezentowania informacji w treści polityki prywatności powinno mieć schemat blokowy dla zachowania jej przejrzystości (czytelności). Jest to stosunkowo nowe podejście na rynku, ale w mojej ocenie najbardziej słuszne, w szczególności tam, gdzie procesów przetwarzania danych za pośrednictwem funkcjonalności strony internetowej jest dużo.
Schemat blokowy oznacza, że politykę prywatności dzielimy na procesy przetwarzania danych osobowych. Jeżeli na stronie internetowej identyfikujemy proces składania reklamacji, działania marketingowe (zapis do newslettera), rekrutacje (zbieranie CV), kontakt za pośrednictwem formularza, składanie zamówień to każdy proces powinien zostać osobno ujęty. Ponadto, opisywany proces musi zawierać wszystkie elementy z art. 13 lub 14 RODO (obowiązek informacyjny). Ergo, ile procesów przetwarzania danych osobowych (funkcjonalności) tyle klauzul informacyjnych. Oczywiście elementy zbieżne tj. np.: określenie administratora, danych kontaktowych, informacje o wycofaniu zgody w dalszym ciągu mogą być prezentowane zbieżnie (w jednym miejscu – w górnej części polityki prywatności) dla wszystkich procesów przetwarzania danych.
Podkreślenia wymaga, że wyżej opisany model w przeważającej mierze dotyczy stron internetowych oferujących użytkownikowi wiele funkcjonalności – nie musi być stosowany tam, gdzie strona internetowa ogranicza się do formularza kontaktowego. Co nie oznacza, że mamy przyzwolenie na ścianę tekstu i chaos informacyjny. Polityka prywatności w dalszym ciągu powinna być ustrukturyzowana m.in. poprzez zachowanie schematu prezentowania informacji zawartego w art. 13 lub 14 RODO (obowiązek informacyjny).

PROBLEM IV

Prawny, formalny język używany w polityce prywatności.

Trzeba pamiętać, że Polityka Prywatności jest kierowana do użytkownika a nie absolwenta wydziału prawa lub specjalisty w dziedzinie ochrony danych osobowych. Polityka prywatności ma być przede wszystkim zrozumiała i komunikatywna. Podmiot danych powinien otrzymać informacje w taki sposób, aby bez konieczności zasięgania opinii profesjonalisty lub reseach'u w internecie zrozumiał w jaki sposób przetwarzane są jego dane osobowe – co się z nimi, de facto, dzieje po tym jak je przekaże lub zostaną pozyskane przez administratora.

Dodatkowo, dobrą praktyką jest używanie przykładów oraz praktycznych opisów sytuacji związanych z przetwarzaniem, w szczególności przy wskazywaniu celów i podstaw przetwarzania, jak również przy opisywaniu przetwarzania danych na podstawie prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f) RODO) – tutaj administrator ma obowiązek opisania działań jakie będą wykonywanie na danych przetwarzanych na podstawie prawnie uzasadnionego interesu.

Podsumowanie

Powyższe opracowanie to oczywiście generalne ujęcie kluczowych problemów jakie wysuwają się na pierwszy plan przy analizowaniu obecnych na rynku polityk prywatności. Problemów jest więcej i często szczególnych - związanych z konkretnymi procesami przetwarzania danych na stronach internetowych. Tym niemniej, od czegoś trzeba zacząć a stosowanie wyżej opisanych praktyk to solidna podstawa dla wdrożenia polityki prywatności „zgodnej z RODO".

Paweł Wojciechowski – adwokat, specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.