Warszawa, dn. 22.04.2021 r.

Jak stworzyć stronę internetową zgodną z RODO?
Część 1 - regulaminy.

Zajmując się doradztwem z zakresu ochrony danych osobowych na pewno weryfikowaliście klauzule informacyjne, opiniowaliście umowy powierzenia czy wykonywaliście audyt funkcjonującej strony internetowej. Co jednak możemy zrobić, gdy takiej strony nie ma, a dopiero powstaje? Mam nadzieję, że poniższy artykuł pozwoli uporządkować zawartość dokumentów, w których przedsiębiorca powinien zamieścić odpowiednie obowiązki informacyjne, nakazane przepisami prawa.

Regulaminy, obowiązki informacyjne, banery cookies – czy są potrzebne?

Tworząc stronę internetową musimy zastanowić się, co zostanie na niej umieszczone, a w związku z tym jakie informacje bądź opis działania mechanizmów musimy na niej umieścić. Część informacji nie będzie związana z RODO, a wynika z odrębnych przepisów. Dla przykładu przedsiębiorca jest zobowiązany do spełnienia obowiązków informacyjnych, o których można przeczytać np. w art. 206 i 374 Kodeksu Spółek Handlowych (jeżeli mamy do czynienia z osobą prawną), art. 20 ustawy Prawo Przedsiębiorców (uPP), art. 5-8 ustawy o Świadczeniu Usług Drogą Elektroniczną (uŚUDE), czy art. 12 ustawy o Prawach Konsumenta (uPK) - w przypadku prowadzenia sklepu on-line).

Przepisy mnożą się, można je wymieniać w nieskończoność, a w rzeczywistości wchodząc na stronę internetową nie czujemy się przytłoczeni wieloma dokumentami, które wskazywałyby spełnienie poszczególnych obowiązków. Dlaczego? Ponieważ część obowiązków związanych z identyfikacją podmiotu prowadzącego stronę (czyli zamieszczeniem pełnej nazwy wraz z danymi identyfikującymi) powtarza się w poszczególnych przepisach np. art. 20 ust. 3 uPP nakazuje przedsiębiorcy oferującemu towary lub usługi w wskazać: firmę, NIP, siedzibę albo adres, natomiast art. 12 ust. 1 pkt 2) oraz 3) uPK zobowiązuje do wskazania firmy, organu, który zarejestrował działalność gospodarczą, numeru, pod którym podmiot został zarejestrowany, adresu przedsiębiorstwa, adresu e-mail, numeru telefonu czy faxu. Dla osób doradzających w zakresie ochrony danych osobowych czy IODów brzmi znajomo? Oczywiście! W końcu zgodnie z art. 13 RODO administrator danych podczas pozyskiwania danych osobowych informuje o swojej tożsamości oraz danych kontaktowych.

Tworząc stronę internetową często spełniamy wyżej wskazane obowiązki w kilku głównych dokumentach, tj. w:

1) regulaminie strony internetowej,
2) polityce prywatności,
3) polityce plików cookies.

Regulamin

Co powinien zawierać regulamin? To już zależy od zawartości strony internetowej i oferowanych na niej usług. Najczęściej w regulaminie zamieszczane są treści, które musimy wstawić na podstawie różnych przepisów, o czym wyżej wspomniałem. Nie zastanawiajmy się długo od czego powinniśmy zacząć tworząc regulamin. Zacznijmy od pełnych danych identyfikujących właściciela strony internetowej, a następnie zajrzyjmy np. do art. 8 ust. 3 uŚUDE. Według niego należy wskazać rodzaje

i zakres usług świadczonych drogą elektroniczną – i wiedza o usługach przyda się następnie w polityce prywatności, do której omówienia przechodzimy.

Polityka prywatności

Konsumenci są co raz bardziej świadomi i sprawdzają treści zamieszczonych dokumentów na stronie. Może to wynikać z ilości banerów, którymi na co dzień każdy z nas jest atakowany wchodząc w świat on-line, a także głośnych wycieków danych z popularnych serwisów internetowych, czyli po prostu z dbania o bezpieczeństwo swoich danych osobowych oraz swoich finansów osobistych. Przed zapisaniem się na newsletter (np. skuszeni kodem rabatowym), czy dokonaniem zakupu na nieznanej stronie internetowej użytkownicy strony chętnie weryfikują podlinkowaną politykę prywatności, aby dowiedzieć się, komu przekazują swoje dane osobowe. Czytelna i dobrze napisana polityka prywatności odzwierciedlająca sposób działania organizacji budzi zaufanie. Dlatego tworząc ją kierujmy się naszymi odbiorcami, do kogo się zwracamy, jednocześnie pamiętając o zasadzie przejrzystości - czasami lepiej jest napisać ją w sposób mniej formalny, aby treść była zrozumiała.

Nigdzie nie wskazano, co powinna zawierać polityka prywatności, więc może to być pewne ułatwienie dla nas, ponieważ przed naszymi oczami widnieje *tabula rasa* do uzupełnienia. Myślę, że dobrą praktyką jest zamieszczenie w jej treści informacji o:

1) bezpieczeństwie danych osobowych, czyli zasadach, którymi się kierujemy;
2) sposobie przetwarzania danych osobowych.

Podając informację na temat zasad bezpieczeństwa możemy poinformować użytkownika naszej strony internetowej np. o:

a) posiadanym certyfikacie SSL zapewniającym poufność transmisji danych przesyłanych przez Internet;
b) stosowanej komunikacji oraz o tym, że nigdy telefonicznie, za pośrednictwem sms lub e-mail nie prosimy o podanie hasła;
c) gdzie można zgłaszać incydenty bezpieczeństwa związane z naszym serwisem, czy podejrzane wiadomości e-mail podmiotów podszywających się pod nasz sklep i chcących wyłudzić dane;
d) posiadanych kopiach zapasowych i możliwości odtworzenia danych;
e) posiadanym rozwiązaniu chroniącym przed atakami DDoS.

W przypadku informowania o sposobie przetwarzania danych osobowych możemy krótko wspomnieć o zasadach, którymi się kierowaliśmy projektując poszczególne usługi, np.:

a) zasadzie minimalizacji,
b) zasadzie ograniczenia przechowywania danych,
c) sposobie odwołania zgody, jeżeli została wyrażona,

czyli w polityce zapewniamy użytkownika strony przykładowo o tym, że nasze usługi zbierają tylko te dane osobowe, bez których nie mamy możliwości świadczenia konkretnej usługi. Zgodnie ze wskazaną zasadą adres e-mail jest niezbędny w celu otrzymania newslettera, ale dzień i miesiąc urodzin już jest fakultatywny. Niemniej zostawiając informację taką informację klient może liczyć na dodatkowe zniżki w sklepie w dniu swoich urodzin, o czym go poinformujmy. Polityka prywatności jest dobrym miejscem do rozwinięcia wszelkich dodatkowych informacji, które mogą być przydatne dla użytkownika strony www.

Dodatkowo możemy przedstawić sposoby przetwarzania danych osobowych na naszej stronie internetowej, czyli do danej usługi opisanej w regulaminie wskażmy obowiązek informacyjny w przystępnej formie. Coraz popularniejsze wydają się tabelki, które porównują sposób przetwarzania

danych dla konkretnych usług. Obowiązek informacyjny i tak jest spełniany każdorazowo, ale w jednym miejscu możemy podsumować w kreatywny sposób, co robimy z danymi osobowymi użytkownika strony internetowej.

Polityka plików cookies

Czy jest nam potrzebna polityka cookies? Na tak postawione pytanie należy odpowiedzieć pozytywnie. Z ciasteczek na pewno będziemy korzystać na naszej nowej stronie, choć pewnym można być jedynie śmierci i podatków. Dodatkowo możemy korzystać z innych technologii, o których także należałoby wspomnieć, przykładowo o geolokalizacji. W przeciwieństwie do pozostałych dokumentów obowiązek zamieszczenia informacji o korzystaniu z plików cookies oraz innych technologii wynika wprost z przepisów, a mianowicie z art. 173 prawa telekomunikacyjnego, zgodnie z którym:

1. Przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego jest dozwolone, pod warunkiem że:
1) abonent lub użytkownik końcowy zostanie uprzednio bezpośrednio poinformowany w sposób jednoznaczny, łatwy i zrozumiały, o:
    a) celu przechowywania i uzyskiwania dostępu do tej informacji,
    b) możliwości określenia przez niego warunków przechowywania lub uzyskiwania dostępu do tej informacji za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi;
2) abonent lub użytkownik końcowy, po otrzymaniu informacji, o których mowa w pkt 1, wyrazi na to zgodę.

Dlatego pamiętajmy, aby umieścić informację o cookies, stosowanych wtyczkach czy innych narzędziach społecznościowych, geolokalizacji lub innych technologiach, które potrzebują uzyskać dostępu do informacji o użytkowniku naszej strony.

Do obsługi plików cookies potrzebujemy odpowiednich narzędzi, aby móc nimi zarządzać, czyli pobierać zgody wyrażone przez użytkowników strony i umożliwić ich wycofanie, a w przypadku niewyrażenia – uniemożliwić wgrywanie się ciasteczek na urządzenie użytkownika. Temat zgód na pliki cookies został poruszony w innych artykułach na naszym blogu, np. pod adresem https://www.isecure.pl/blog/ciasteczko-po-irlandzku-czyli-irlandzki-organ-nadzorczy-o-plikach-cookies/ można znaleźć informację o raporcie irlandzkiego organu ochrony danych osobowych, który zbadał strony przedsiębiorców, informując o błędnych praktykach i jednocześnie wskazując na te poprawne; oraz pod adresem https://www.isecure.pl/blog/pliki-cookies-po-polsku/ gdzie kolega z Zespołu iSecure Bartosz Migas podsumował zagadnienia związane z ciasteczkami.

Wspomniany wyżej przepis prawa telekomunikacyjnego może ulec zmianie ze względu na nową ustawę Prawo komunikacji elektronicznej, której przyjęcie ma być wdrożeniem dyrektywy o Europeskim Kodeksie Łączności Elektronicznej. O cookies według nowej ustawy można przeczytać w naszym artykule znajdującym się na stronie: https://www.isecure.pl/blog/marketing-i-cookies-w-projekcie-prawo-komunikacji-elektronicznej/.

Dwa zdania na zakończenie części pierwszej.

Często polityka prywatności stanowi część regulaminu. Moim zdaniem te dwa dokumenty należy rozdzielić, podobnie jak politykę plików cookies nie wstawiałbym do polityki prywatności. W zależności od wielości usług i skomplikowania strony internetowej dokumenty mogą być znacząco rozbudowane (i się rozrastać), a pamiętajmy by zagwarantować czytelność tych dokumentów dla naszego dobra i naszych klientów. Ponadto dokumenty powinny być łatwe do wyszukania na stronie internetowej, dlatego warto zamieszczać linki do osobnych podstron np. na dole strony internetowej, aby niezależnie od otwartej zakładki podstawowe informacje zawsze znajdowały się w belce na dole, lub w dedykowanej zakładce np. o bezpieczeństwie sklepu on-line.

W tej części wskazaliśmy podstawowe dokumenty które należy przemyśleć tworząc stronę internetową zgodnie z RODO oraz polskimi przepisami. Jakie inne czynności należy przedsięwziąć, czyli o planowaniu strony (privacy by design), formularzach umieszczanych na stronie czy zgodach – napiszemy w kolejnych odsłonach „Jak stworzyć stronę internetową zgodną z RODO?", cyklu dla Inspektorów Ochrony Danych dostępnym w mediach społecznościowych pod hashtagiem **#iWarsztatIOD.** Już dzisiaj serdecznie zapraszam do kontynuacji artykułu.

Przemysław Siarka, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.