

Prawo dostępu do danych – w oczach EROD

Jesteś klientem, konsumentem, osobą fizyczną, która zostawia swoje dane osobowe u przedsiębiorcy? Wpisujesz swoje imię, nazwisko, adres zamieszkania w formularzach na stronie www sklepu, pozostawiasz swoje dane w firmach, w umowie, u lekarza. A może jesteś przedsiębiorcą, który zbiera dane osobowe w związku z oferowanymi usługami, sprzedają towarów lub po prostu zbierasz dane swoich pracowników jako pracodawca? Tak naprawdę to nie ma znaczenia. Jestem pewny, że bez względu na to po której stronie się znajdujesz – udostępniasz swoje dane, bądź je zbierasz - słyszałeś o RODO. W końcu trafiłeś na ten wpis i interesuje Cię realizacja prawa dostępu do danych. Czyli albo chcesz skorzystać ze swojego prawa i dowiedzieć się jakie dane posiada firma XYZ, albo otrzymałeś taki wniosek od osoby zainteresowanej dostępem do swoich danych.

Europejska Rada Ochrony Danych (EROD) udostępniła wytyczne do konsultacji publicznych przedstawiając różne aspekty prawa dostępu do danych https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_pl, o których napiszę poniżej, co pozwoli przybliżyć omawiane zagadnienie.

Czym jest prawo dostępu do danych?

Prawo dostępu do danych osobowych ma na celu dostarczenie odpowiedzi osobie zainteresowanej (klientowi, konsumentowi), czy administrator danych (firma XYZ) posiada w swoich zbiorach dane osobowe pytającego. Dzięki otrzymanej odpowiedzi wnioskodawca będzie mógł zweryfikować legalność przetwarzanych danych, ich aktualność oraz żądać informacji o samym przetwarzaniu (np. w jakim celu dane są przechowywane, jak długo, i jakie dane posiada przedsiębiorca będący administratorem danych).

W jaki sposób przedsiębiorca spełnia prawo dostępu do danych?

Po weryfikacji wnioskodawcy administrator danych powinien sprawdzić w systemach informatycznych oraz w zbiorach zwykłych czy posiada dane osoby pytającej. Następnie administrator odpowiada na zadane pytanie bądź dostarcza wnioskodawcy informacji o nim w postaci kopii danych. Kopia powinna być dostarczona w sposób umożliwiający jej odtworzenie przez wnioskującego, w formie papierowej lub elektronicznej. Gdy ilość danych jest bardzo duża i trudne byłoby zrozumienie przekazanych informacji – zwłaszcza w kontekście danych zebranych online, najbardziej odpowiednim środkiem według EROD może być udostępnienie danych warstwowo, co ułatwi ich zrozumienie, niemniej powinny być przesłane w jednym terminie.

Jednocześnie pamiętajmy, że żądanie dostępu do danych nie może naruszać prawa lub wolności innych osób. Osoba, która wysłała zapytanie do administratora danych (przedsiębiorcy) może żądać podania informacji dotyczących jedynie jej osoby. Inne żądania mogą być odrzucone. Podobnie żądania ewidentnie nieuzasadnione lub nadmierne.

Pozyskanie kopii przetwarzanych danych u przedsiębiorcy nie powinno być traktowane jako oddzielne prawo dostępu do danych i pozyskania ich kopii. Przy czym należy pamiętać, że zgodnie z art. 15 ust. 3 RODO i wskazówkami EROD, w przypadku zagubienia lub uszkodzenia przez wnioskodawcę otrzymanej kopii danych, przedsiębiorca może pobrać opłatę w rozsądnej wysokości za wydanie kolejnej kopii danych.

Przekazując kopię danych pamiętajmy o zabezpieczeniach. EROD zaleca przekazywanie danych osobowych listem poleconym, w przypadku formy papierowej albo w sposób szyfrowany,

zabezpieczony hasłem, gdy dane przekazywane są elektronicznie. Poziom środków bezpieczeństwa oczywiście powinien być uzależniony od rodzaju udostępnianych danych osobowych.

Kroki wskazane przez EROD.

EROD w swoich wytycznych podpowiada następujące kroki dla administratorów danych:

1. Zweryfikuj, czy wniosek dotyczy danych osobowych,
2. Zweryfikuj, czy wniosek dotyczy osoby, która go składa, bądź osoby uprawnionej do działania w cudzym imieniu,
3. Zweryfikuj, czy mają zastosowanie inne niż RODO przepisy regulujące dostęp do określonych danych osobowych,
4. Zweryfikuj, czy wniosek wchodzi w zakres art. 15 RODO,
5. Zweryfikuj, czy wnioskodawca chce uzyskać dostęp do całości lub części przetwarzanych danych.

Przedsiębiorca chcąc doprecyzować żądanie czy informację od kogo wniosek pochodzi, będzie zmuszony doprecyzować powyższe kwestie przez zadanie dodatkowych pytań wnioskodawcy. Dlatego będąc wnioskodawcą należy pamiętać o współpracy z administratorem, do którego wysłany został wniosek o dostęp do danych.

Nieprawidłowy adres e-mail, na który przyszedł wniosek.

Nigdzie nie jest wskazane jak powinien wyglądać formularz prawa dostępu do danych, czy jak powinien być zbudowany adres e-mail, na który osoby zainteresowane mogą wysłać żądanie. Brak takich wymagań potwierdza również EROD. Niemniej co powinien zrobić administrator danych (przedsiębiorca) po otrzymaniu wniosku na adres e-mail swojego pracownika niezajmującego się obsługą żądań (nieznającego zasad wynikających z RODO)? Z jednej strony EROD wskazuje, że administrator danych nie jest zobowiązany do podjęcia działań wynikających z żądania wysłanego na błędny adres e-mail, jeżeli udostępnił odpowiedni kanał komunikacyjny w tym celu. A z drugiej strony EROD zachęca administratorów do zapewnienia sprawnej wewnętrznej komunikacji między pracownikami, aby wnioski błędnie adresowane były forwardowane i dochodziły do odpowiedniej komórki w firmie zajmującej się ich realizacją. Szczególnie należy pamiętać, gdy realizacją wniosków zajmuje się jedna osoba, aby znaleźć zastępstwo w przypadku jej nieobecności w biurze. Ponadto EROD zaznacza, że wniosek skierowany na nieprawidłowy (niededykowany) adres e-mail, nie usprawiedliwia przedłużenia terminu na odpowiedź.

Potrzeba identyfikacji wnioskodawcy.

Co powinien zrobić administrator danych, który otrzymał żądanie dostępu do nagrania z monitoringu, ale nie może zidentyfikować wnioskodawcy? Tutaj również otrzymamy od EROD nieścisłą odpowiedź. W swoich rozważaniach EROD zaznacza, że często takie żądanie może wiązać się z koniecznością pozyskania od wnioskodawcy dodatkowych danych osobowych. Natomiast art. 11 RODO usprawiedliwia administratora z niepodjęcia działań i braku realizacji wniosku, dzięki zwolnieniu go z obowiązku pozyskania dodatkowych danych osobowych. Gdy nie ma możliwości zidentyfikowania wnioskodawcy, nie można zrealizować praw wynikających z RODO, w tym prawa dostępu do danych. Jednakże gdy osoba zainteresowana dostarczy dodatkowe informacje pozwalające ją zidentyfikować – administrator nie może odmówić ich przyjęcia i powinien dążyć do realizacji wniosku. EROD podkreśla, że administrator też może żądać podania dodatkowych informacji niezbędnych do potwierdzenia tożsamości wnioskodawcy, jednak muszą być to informacje usprawiedliwione pozwalające na identyfikację wnioskodawcy. EROD wskazuje na dobrą praktykę jaką jest posiadanie

odpowiednich procedur umożliwiających złożenie wniosku, weryfikację osoby i dostarczenie odpowiedzi (ew. kopii danych).

Przykłady dostępu do danych podane przez EROD.

1. Wniosek o dostęp do danych przesłany na główny adres e-mail.

Administrator XYZ podaje na stronie internetowej oraz w polityce prywatności dwa adresy e-mail - ogólny: kontakt@xyz.com oraz punkt do składania wniosków dot. danych osobowych: zapytania@xyz.com. Dodatkowo Administrator XYZ wskazuje na swojej stronie, że w celu złożenia wniosku o dostęp do danych należy napisać na adres: zapytania@xyz.com. Wnioskodawca, będący klientem sklepu online, kieruje jednak swoje żądanie na adres: kontakt@xyz.com zamiast na dedykowany: zapytania@xyz.com.

W takim przypadku Administrator XYZ powinien dołożyć wszelkich uzasadnionych starań, aby jego pracownicy przekierowali żądanie pod właściwy adres e-mail, w celu dalszego procesowania wniosku i udzielenia odpowiedzi w terminach przewidzianych przez RODO.

2. Weryfikacja osoby składającej wniosek.

Pani Y zakładając konto w sklepie internetowym podała swój adres e-mail i login (nazwę użytkownika). Następnie wysłała zapytanie do sklepu czy przetwarza jej dane osobowe, a jeżeli tak to prosi o udzielenie informacji zgodnie z art. 15 RODO. Pracownik sklepu w odpowiedzi na żądanie poprosił o przesłanie dowodu osobistego w celu potwierdzenia tożsamości użytkowniczki sklepu.

EROD uznał to za nieuzasadnione działanie sklepu prowadzące do niepotrzebnego gromadzenia danych.

Słowo na zakończenie.

Na powyższych przykładach widać, że:

- należy dbać o podnoszenie świadomości wśród pracowników,
- szkolić swoich pracowników z zakresu RODO i bezpiecznego przetwarzania danych osobowych, aby wiedzieli, jak powinni się zachować, nawet gdy nie są osobami dedykowanymi do obsługi żądań klientów,
- posiadać odpowiednie procedury obsługi wniosków.

Administrator danych posiadający wykwalifikowanych pracowników i odpowiednie procedury może mieć pewność, że nie ominie go żaden wniosek, na który musi odpowiedzieć w ciągu miesiąca, dzięki czemu uniknie administracyjnej kary finansowej.

Przemysław Siarka – specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.