Warszawa, 11.05.2022 r.

Czy muszę udostępniać dane na żądanie osoby fizycznej? Jeżeli tak, to jak bezpiecznie zrealizować prawo dostępu do 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. Konsultacje zostały zakończone, pierwszą część wytycznych opisałem w poprzednim artykule https://www.isecure.pl/blog/prawo-dostepu-do-danych-w-oczach-erod/, teraz zapraszam na drugą część.

Na co powinieneś zwrócić uwagę obsługując wniosek dostępu do danych?

Za wytycznymi ERODu powtórzmy ogólne zasady prawa dostępu do danych. Co jeszcze powinieneś robić poza identyfikacją wnioskującego oraz żądania czy weryfikacji jego osoby? Zapamiętaj:

- Nie zawężaj wniosku o dostęp do danych.
- Podawaj wnioskodawcy faktyczne informacje o jego danych osobowych.
- Zapewnij środki organizacyjne umożliwiające sprawne spełnienie żądania, np. stwórz procedurę.
- Przekazuj dane osobowe w sposób bezpieczny (np. listem poleconym lub zahasłowanym mailem)

Dostałeś ogólne żądanie dostępu do danych? Możesz poprosić o doprecyzowanie, jednak zapamiętaj, aby nigdy go nie zawężać. Ogólny wniosek powinien być rozpatrywany jako żądanie obejmujące wszystkie dane osobowe, chyba że wnioskodawca wyraźnie ograniczył żądanie do konkretnego podzbioru.

Czy można składać żądanie dostępu do danych za pośrednictwem osób trzecich?

Można. Chociaż prawo dostępu do danych powinno być wykonywane przez osoby, których dane dotyczą (ponieważ to jest ich sprawa), niemniej możliwe jest złożenie wniosku przez osobę trzecią (pełnomocnika) w imieniu osoby zainteresowanej, której dane przetwarzamy w systemach. Wówczas będziemy musieli zweryfikować tożsamość pełnomocnika, aby nie udostępnić danych osobowych osobie nieupoważnione. Najczęściej taka sytuacja będzie występowała , gdy osoba której dane przetwarzamy:

- skorzysta z usług profesjonalisty (np. reprezentuje ją adwokat, radca prawny),
- jest niepełnoletnia i w jej imieniu wystąpi rodzic lub inny opiekun prawny,
- zmarła.

Przy czym adwokat bądź radca prawny, jako profesjonalista, jest zawodem zaufania publicznego i potwierdzenie wykonywanego zawodu łatwo możemy znaleźć w rejestrach odpowiedniej rady. Natomiast zgodnie z motywem 27 RODO – przepisy rozporządzenia nie mają zastosowania do danych osobowych osób zmarłych. Jednak w tym ostatnim przypadku należy pamiętać, że w przypadku korespondencji zmarłego Twoja firma może przetwarzać dane osób żyjących, a takie dane nadal wymagają ochrony.

Sposoby zapewnienia dostępu do danych osobowych

Przede wszystkim administratorzy danych osobowych muszą pamiętać o właściwej procedurze. To ułatwi im udokumentowanie swojego podejścia i wykazanie w jaki sposób wybrane środki mają dostarczyć niezbędnych informacji zgodnie z art. 15 RODO. Należy też

się zastanowić, czy zawsze zapewnienie prawa do stępu do danych jest równoznaczne z dostarczeniem ich kopii. EROD wskazuje, że administrator może udostępnić dane osobowy wnioskodawcy zarówno jako przekazanie informacji ustnej jak i przez zapewnienie wglądu do akt, umożliwienie dostępu na miejscu bądź zdalnie bez możliwości pobrania tych danych. Przy czym udzielenie dostępu w inny sposób niż udostępnienie kopii danych nie wyklucza prawa wnioskodawcy do posiadania kopii danych (chyba, że zrzeka się tego prawa).

Ograniczenie prawa dostępu do danych

Prawo dostępu do danych podlega ograniczeniom wynikającym z:

- art. 15 ust. 4 RODO – prawa i wolności innych osób, oraz
- art. 12 ust. 5 RODO – oczywiście bezpodstawne lub nadmierne żądanie.

Poza powyższymi ograniczeniami (i możliwymi odstępstwami, które mogą wprowadzić indywidualnie kraje członkowskie), nie ma innych, które usprawiedliwiałyby bierność administratora danych. Nawet jeżeli zebranie żądanych informacji czy danych kosztowałoby dużo nieproporcjonalnego wysiłku administratora. A wnioskodawca nie musi argumentować powodu korzystania z prawa dostępu do swoich danych.
Najbardziej typowym przypadkiem ograniczenia prawa dostępu do danych jest prawo do ochrony danych innych osób. Administrator powinien ocenić i udokumentować wykonaną analizę związaną z każdym ograniczeniem, o czym należy pamiętać. Trzeba też brać pod uwagę prawdo do prywatności korespondencji, tajemnicy handlowej czy własności intelektualnej. EROD wyraźnie podkreśla, że administrator danych musi być w stanie wykazać, że w konkretnej sytuacji prawa lub wolności innych osób zostałyby faktycznie naruszone.

Przykłady dostępu do danych podane przez EROD

1. Dostęp do danych osobowych z rekrutacji.

Z pewnością częste są sytuacje, gdy w trakcie rekrutacji przychodzi do Ciebie kandydat i przekazuje swoje dane osobowe w CV oraz w liście motywacyjnym. Następnie Ty lub Twój pracownik zapraszasz osobę na rozmowę z której sporządzasz notatki na komputerze w celu udokumentowania przebiegu rozmowy. A czy otrzymałeś po rozmowie żądanie kandydata dostępu do jego danych osobowych, które zostały zebrane w toku postępowania?
Zgodnie z zaproponowanymi wytycznymi firma powinna udostępnić dane osobowe otrzymane w CV i liście motywacyjnym, a dodatkowo streszczenie rozmowy kwalifikacyjnej łącznie z poczynionymi subiektywnymi komentarzami – jeżeli dotyczą kandydata. Wynika to m. in. z wyroku TSUE, który stwierdził, że takie informacje też stanowią dane osobowe, gdy dotyczą osoby składającej wniosek (wyrok z 20 grudnia 2017 r. C-434/16).

2. Czy muszę przekazać wszystkie dane osobowe, czy tylko te, które wnioskodawca sam przekazał?

Prawo dostępu do danych obejmuje zarówno dane otrzymane jak i pochodne (wywnioskowane, dodatkowo samodzielnie zebrane lub stworzone). Inaczej wygląda inne prawo osoby fizycznej – prawo do przeniesienia danych, które obejmuje wyłącznie dane dostarczone przez osobę żądającą ich przeniesienia. Jednak w przypadku prawa dostępu do danych, osoba wnioskująca o dane powinna otrzymać nie tylko te, które przekazała administratorowi danych, ale także te, które administrator sam wytworzył.

3. Czy muszę informować o konkretnych odbiorcach danych osobowych czy mogę powiadomić o ogólnej kategorii odbiorców?

Według EROD należy pamiętać o poszanowaniu zasady transparentności. Na początku wypełniając obowiązek informacyjny z art. 13 lub 14 RODO możemy nie znać konkretnych hoteli czy biur podróży, którym dane będą udostępnione w związku z np. podróżą służbową. Jeżeli później po odbyciu podróży pracownik korzystając z dostępu do danych poprosi o ujawnienie informacji o odbiorcach swoich danych, zgodnie z art. 15 ust. 1 lit. c) RODO, administrator danych udzielając odpowiedź powinien wskazać konkretne biuro podróży czy dane hotelu, które otrzymały dane pracownika. Czyli według EROD staramy się przekazać jak najbardziej konkretne informacje.

Słowo na zakończenie

Administratorzy danych osobowych codziennie otrzymują żądania dostępu do danych wnioskodawców lub prośby o uzyskanie kopii. A to tylko jedno z wielu praw osób, których dane są przetwarzane. Dlatego, aby utrzymać porządek i rozliczalność, dobrym nawykiem będzie prowadzenie ewidencji takich żądań. Wówczas mamy pełną wiedzę o żądaniach dostępną w każdym momencie – które zostało zrealizowane, w jaki sposób, w jakim czasie, a jeżeli nie zostało zrealizowane, to z jakiego powodu. Posiadając taką ewidencję będziemy czuć się pewniej podczas kontroli Urzędu i nie będziemy musieli gorączkowo przeszukiwać wszystkich skrzynek pocztowych.
Jednak nie każda procedura czy ewidencja zastąpi świadomość pracowników. Pamiętaj o szkoleniach i instruowaniu pracowników jak powinni postępować w danej sytuacji. Aby po otrzymaniu wniosku z prośbą o dostęp do danych przekazali ją niezwłocznie do Twojego inspektora ochrony danych lub jednostki odpowiedzialnej za realizację żądań. Czasami odruchowo pracownik bez zweryfikowania osoby pytającej może udzielić odpowiedzi, a gdy ujawnimy dane osobie nieuprawnionej wówczas dochodzi do naruszenia poufności danych. Dlatego należy uważać komu udostępniamy informacje i czy robimy to w sposób bezpieczny.

Przemysław Siarka - specjalista ds. ochrony danych osobowych w iSecure sp. z o.o.