CSO

Jakie działania powinniśmy podjąć po naruszeniu ochrony danych osobowych?

RODO narzuca na przedsiębiorców wiele obowiązków mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych. Ich wdrożenie przez przedsiębiorców jest absolutnie niezbędne, ale nie gwarantuje 100-proc. ochrony przed niepożądanymi zdarzeniami. Ustawodawca przewidział zatem dużo działań, które należy podjąć na wypadek ewentualnego wycieku danych. Oto ich opis.

W ostatnim czasie otrzymujemy coraz więcej informacji o naruszeniach ochrony danych osobowych, w tym także o incydentach z zakresu cyberbezpieczeństwa. Trzeba wyraźnie podkreślić, że część z nich jest spowodowana niewdrożeniem lub niewłaściwym wdrożeniem stosownych środków, ale istnieją też takie, które są efektem działań zorganizowanych grup przestępczych. W ostatnich latach świat usłyszał o takich sprawach jak ransomware Petya. Były to początkowo ataki na infrastrukturę IT przedsiębiorców na Ukrainie, które w późniejszym czasie rozprzestrzeniły się również na inne kraje. Innym przykładem cyberataku był wyciek danych z serwisu randkowego Ashley Madison w Kanadzie, czy też z polskiego serwisu morele.net.

Co zrobić, gdy jednak dojdzie do wycieku?

Incydenty związane z wyciekiem danych osobowych udowodniły, że w rzeczywistości nie istnieją takie rozwiązania, które mogłyby całkowicie im zapobiec. Każdy z przedsiębiorców powinien być na nie przygotowany i dlatego tak ważne jest, aby we własnym zakresie ustalił wewnętrzne procedury umożliwiające szybkie i efektywne reagowanie na tego typu zdarzenia.

Każdy przedsiębiorca już na etapie przeprowadzanego audytu RODO powinien ustalić, w których obszarach przetwarza dane osobowe klientów, kontrahentów czy też pracowników. Tylko te obszary będą przedmiotem naszego zainteresowania w kontekście podjęcia ewentualnych działań po wycieku danych. Oceny każdego zdarzenia powinniśmy dokonać z punktu widzenia interesu grupy potencjalnie najbardziej zagrożonej jego skutkami, a zatem osób, których dane wyciekły poza naszą instytucję.

Po pierwsze, zgłoszenie do UODO

W przypadku naruszenia ochrony danych osobowych administratorzy są zobowiązani w miarę możliwości, bez zbędnej zwłoki, aczkolwiek nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia, zgłosić je Urzędowi Ochrony Danych Osobowych (UODO), chyba że istnieje małe prawdopodobieństwo, aby naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób, których dane wyciekły.

Do zgłoszenia o wycieku danych osobowych – przekazanego organowi nadzorczemu po upływie 72 godzin – dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenia dokonujemy za pośrednictwem formularza dostępnego na stronie UODO, które powinno co najmniej opisywać charakter naruszenia, zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji, podawać możliwe konsekwencje naruszenia, opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opisywać środki, aby zminimalizować jego ewentualne negatywne skutki.

Co istotne, w ramach niektórych operacji na danych osobowych będziemy występować jako podmiot przetwarzający na skutek uprzednio zawartej z odrębnym podmiotem umowy powierzenia. W tych sytuacjach RODO nakłada na nas obowiązek zgłoszenia zdarzenia administratorowi.

Po drugie, ocena skutków cyberataku

Ocena ewentualnych skutków naruszeń jest absolutnie kluczowa dla ustalenia odpowiedniej ścieżki działania po wycieku danych. Należy zwrócić uwagę, że RODO nakłada na przedsiębiorców obowiązek dokumentowania wszelkich naruszeń, w tym jego okoliczności, jego skutków, a także podjętych przez nas działań zaradczych. Większość przedsiębiorców zapomina, iż w pierwszej kolejności po wycieku danych należy podjąć te działania, które mają na celu zapobiegnięcie dalszemu wyciekowi danych oraz należyte zabezpieczenie interesu osób, których dane są przedmiotem zdarzenia. Aspekt formalny powinien być realizowany niezwłocznie, ale jest on zdecydowanie mniej istotny niż same działania zaradcze. Sprawdzoną metodą jest zatem dokonanie przez przedsiębiorcę wstępnego zgłoszenia incydentu do UODO wraz ze wskazaniem terminu, w którym będziemy w stanie uzupełnić nasze zawiadomienie.

RODO nakłada na przedsiębiorców obowiązek dokumentowania wszelkich naruszeń, w tym jego okoliczności, jego skutków, a także podjętych przez nas działań zaradczych. Większość przedsiębiorców zapomina, że w pierwszej kolejności po wycieku danych należy podjąć te działania, które mają na celu zapobiegnięcie dalszemu wyciekowi danych oraz należyte zabezpieczenie interesu osób, których dane są przedmiotem zdarzenia. **Aspekt formalny powinien być realizowany niezwłocznie, ale jest on zdecydowanie mniej istotny niż same działania zaradcze. Sprawdzoną metodą jest zatem dokonanie przez przedsiębiorcę wstępnego zgłoszenia incydentu do UODO wraz ze wskazaniem terminu, w którym będziemy w stanie uzupełnić nasze zawiadomienie.**

Bezpośrednio po wycieku danych często padają pytania, czy zdarzenie to na pewno powinniśmy zgłosić. Rzeczywiście, od tego obowiązku możemy odstąpić w sytuacji, gdy istnieje małe prawdopodobieństwo, aby zdarzenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. I takie sytuacje się zdarzają, ale tu należy być nadzwyczaj ostrożnym. Zdecydowanie zalecam zgłaszanie naruszeń do urzędu, wszak ustalenie, że zdarzenie to rodzi jedynie małe ryzyko dla osoby, której dane wyciekły, powinno być poparte szczegółową analizą oraz konkretnymi argumentami przemawiającymi za przyjęciem takiego stanowiska. Każdy przedsiębiorca powinien też we własnym zakresie prowadzić wewnętrzny rejestr naruszeń, w którym takie analizy powinny znaleźć się na wypadek kontroli UODO.

Po trzecie, powiadomienie osób, których dane wyciekły

Jeśli naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator co do zasady o takim naruszeniu bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą. Zawiadomienie to powinniśmy skonstruować jasnym i prostym językiem w tym celu, aby potencjalny odbiorca był w stanie go zrozumieć oraz wykonać wskazane przez nas zalecenia. I tak należy przeanalizować katalog ewentualnych konsekwencji wycieku. Głównie skupiamy się na kradzieży tożsamości, ale to nie jedyne skutki naruszeń. W przypadku danych wrażliwych ich wyciek może doprowadzić do aktów dyskryminacji względem tych osób, a w niektórych sytuacjach także do uniemożliwienia podjęcia zatrudnienia w określonym sektorze. Skutki będą zawsze zależne zarówno od okoliczności zdarzenia, jak i od kategorii danych, które są jego przedmiotem. W niektórych sytuacjach zaleca się również zawiadomienie odpowiednich organów ścigania.

Każdy przedsiębiorca powinien zadbać o jak najwyższy poziom zabezpieczeń, wdrażając w swojej instytucji odpowiednie środki techniczne i organizacyjne. Mimo ich zastosowania, powinien jednak wdrożyć procedurę regulującą prawidłową ścieżkę działania na wypadek wycieku danych, który może mieć miejsce przede wszystkim w związku z przestępczymi działaniami osób trzecich.

Adrian Gajzler, firma doradcza RODO Advisor