

Wrocław, 25 maja 2020 r.

NEWSLETTER

- 2 LATA OD ROZPOCZĘCIA STOSOWANIA RODO

Mijają 2 lata od rozpoczęcia stosowania nowych europejskich przepisów o ochronie danych osobowych. Z tej okazji zapraszamy do lektury newslettera, w którym podsumowujemy najbardziej aktualne tematy z dziedziny ochrony danych osobowych. Nie sposób uniknąć zagadnień związanych z panującą pandemią COVID-19, które budzą wątpliwości wielu przedsiębiorców. W ostatnim czasie obserwujemy także zwiększającą się liczbę postępowań przed polskim organem nadzorczym w związku z wyciekami danych.

I. Praca zdalna

Praca zdalna nigdy jeszcze nie była wykorzystywana na taką skalę jak obecnie. W związku z tym, niejednokrotnie prowadzi to do tego, że dane osobowe są przetwarzane przez pracowników poza siedzibą firmy. To zwiększa ryzyko związane z ich przetwarzaniem. Zatem przedsiębiorcy, jako administratorzy powinni zadbać o ich odpowiednie zabezpieczenie. Przede wszystkim do minimum powinna być ograniczona możliwość wnoszenia dokumentów papierowych. Dodatkowo pracownicy powinni mieć możliwość pracy z domu na służbowych laptopach, nie powinno dochodzić do sytuacji, kiedy pracownicy wykonują zadania z wykorzystaniem swojego prywatnego sprzętu. Dotychczas stosowane zabezpieczenia – np. oprogramowanie antywirusowe – powinny zostać teraz zweryfikowane i ewentualnie zmienione. Pracownicy powinni zostać pouczeni o zadach bezpieczeństwa pracy z domu, w szczególności o tym, aby nie ujawniali haseł, informacji osobom trzecim, w tym również domownikom. Warto wprowadzić wewnętrzne regulacje dotyczące bezpieczeństwa informacyjnego pracy w home office – np. politykę bezpieczeństwa pracy zdalnej.

Jeżeli nie była dokonywana ocena ryzyka dla pracy zdalnej, to przedsiębiorca powinien jak najszybciej podjąć działania w tym zakresie.

II. Postępowania w związku z wyciekiem danych

Prezes Urzędu Ochrony Danych Osobowych informował o wszczęciu kilku postępowań związanych z wyciekiem danych. Postępowania dotyczą zarówno podmiotów publicznych (np. Politechnika Warszawska, Krajowa Szkoła Sądownictwa i Prokuratury), jak i prywatnych (przykładowo SWPS Uniwersytet Humanistycznospołeczny, Panek S.A.).



Do incydentów dochodziło zarówno z powodu ataków pochodzących z zewnątrz, jak i błędów ludzkich, w tym między innymi powstałych w trakcie przesyłania danych.

Urząd Ochrony Danych Osobowych w komunikatach dotyczących naruszeń zwraca szczególną uwagę na termin do zgłoszenia. Zgodnie z przepisami naruszenia należy zgłaszać nie później niż w ciągu 72 godzin od jego stwierdzenia. W przypadku wystąpienia incydentu w zgłoszeniu należy nie tylko podać okoliczności sprawy, ale także zweryfikować, czy wymagane jest powiadomienie osób, których dane dotyczą.

Podkreśla się także, że istotne jest, aby podjąć odpowiednie działania, które pozwolą ograniczyć ewentualne negatywne konsekwencje. Zdarzają się przypadki, że podmiot, u którego wystąpiło naruszenie, podjął decyzję o zwrocie osobom, których dane wyciekły, podstawowych kosztów związanych ze skutkami incydentu.

W trakcie postępowania organ nadzorczy sprawdza informacje o przyjętych środkach technicznych i organizacyjnych, zabezpieczających dane osobowe. Weryfikuje się również przyjęte w organizacji standardy dotyczące regularnego testowania, mierzenia i oceniania skuteczności tych środków.

W związku z tym przedsiębiorcy powinni na bieżąco sprawdzać stan środków zabezpieczających dane osobowe oraz przyjmując odpowiednie procedury na wypadek wystąpienia wycieku danych.

III. Działania podejmowane przez przedsiębiorców w związku z COVID-19

W związku z pandemią COVID – 19, przedsiębiorcy rozważają możliwość podjęcia działań związanych z ograniczeniem rozprzestrzeniania się koronawirusa. Należą do nich m.in. dokonywanie pomiaru temperatury ciała wszystkich osób wchodzących na teren zakładu pracy (pracowników, gości), odbieranie tzw. kwestionariuszy oceny ryzyka epidemiologicznego od osób wchodzących na teren firmy (zawierających pytania m.in. o kontakty z osobami zakażanymi/ w kwarantannie, występowanie objawów charakterystycznych dla COVID-19), czy nawet wykonywanie wszystkim pracownikom (np. po powrocie z przestoju) testów na obecność koronawirusa.

Pomiar temperatury ciała i kwestionariusze

W naszej ocenie wykonywanie pomiaru temperatury ciała, czy odbieranie w/w kwestionariuszy uznać należy za dopuszczalne. Należy jednak pamiętać o tym, że wynik pomiaru temperatury ciała nie powinien być odnotowywany. Podstawą przetwarzania tych danych będzie zapewnienie bezpieczeństwa na terenie zakładu pracy i zapobieganie rozprzestrzenianiu się epidemii (art. 9 ust. 2 lit. b oraz lit. i RODO, art. 6 ust. 1 lit. f RODO).

Testy przesiewowe

Przedsiębiorca jednak nie powinien wykonywać testów przesiewowych, nawet za zgodą pracowników. Takie działania mogą zostać zakwestionowane przez organ nadzorczy w zakresie ochrony danych (Prezes UODO), jako nadmiernie ingerujące w prywatność pracowników.



Jakie się wiążą z tym dodatkowe obowiązki?

W związku z tym, że w/w działania wiążą się z przetwarzaniem danych osobowych, przedsiębiorca powinien, jako administrator danych zadbać o to, aby zrealizowane zostały wszystkie obowiązki wynikające z RODO. Między innymi konieczne jest uzupełnienie rejestru czynności przetwarzania o te procesy, przeprowadzenie dla nich oceny ryzyka, dobranie odpowiednich zabezpieczeń (nie tylko technicznych, ale np. też nadanie upoważnień do przetwarzania danych w tym zakresie osobom, które mają dostęp do takich danych). Konieczne jest też zrealizowanie obowiązku informacyjnego wobec osób, których dane są przetwarzane w związku z przeciwdziałaniem rozprzestrzenianiu się COVID -19.

Aleksandra Baranowska – Górecka
radca prawny

Anna Materla
radca prawny

SDZLEGAL Schindhelm

Kancelaria Prawna Champera, Dubis, Zając i Wspólnicy sp. k.

ul. Kazimierza Wielkiego 3, 50-077 Wrocław

Tel.: +48 71 326 51 40

E-mail: aleksandra.baranowska-gorecka@sdzlegal.pl

E-mail: anna.materla@sdzlegal.pl

www.schindhelm.com