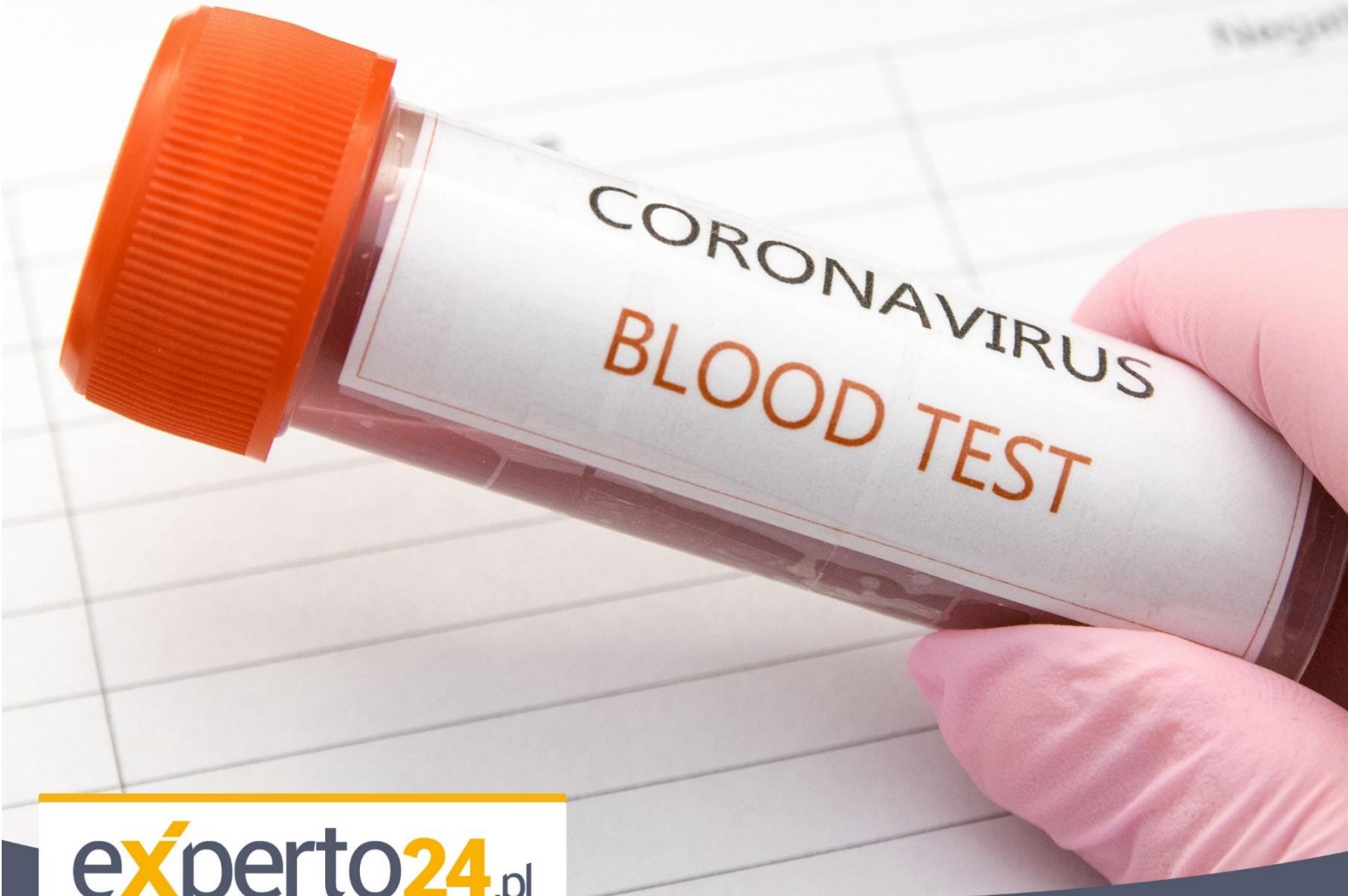
KORONAWIRUS A RODO

– co się zmieniło?



experto24.pl

Spis treści

RODO a koronawirus – oświadczenie Prezesa UODO

RODO nie będzie przeszkodą w realizacji działań związanych z walką z koronawirusem – stanowczo stwierdza Prezes UODO. Nowa specustawa nie stoi więc w sprzeczności z regułami ochrony danych osobowych.

Specjalne uprawnienia GIS i premiera

Pracodawcy są zobligowani do podejmowania działań, wynikających zarówno z zaleceń Głównego Inspektora Sanitarnego, jak i Prezesa Rady Ministrów. Zgodnie bowiem z art. 17 specustawy Główny Inspektor Sanitarny (bądź państwowy wojewódzki inspektor sanitarny – z upoważnienia GIS). Może nakazywać pracodawcom podjęcie określonych czynności zapobiegawczych lub kontrolnych i współdziałanie z innymi organami administracji publicznej oraz organami Państwowej Inspekcji Sanitarnej.

Polecenia przedsiębiorcom w związku z przeciwdziałaniem COVID-19 może wydawać również Prezes Rady Ministrów, na wniosek wojewody, po poinformowaniu ministra właściwego do spraw gospodarki.

Polecenia Prezesa Rady Ministrów przybierają formę decyzji administracyjnej (nie musi ona zawierać uzasadnieni) i są natychmiast wykonalne.

Podstawa przetwarzania danych

Powyższe działania są zgodne z RODO. Wszak RODO uprawnia do przetwarzania danych w związku **z ochroną zdrowia i zapobieganiem rozprzestrzeniania się chorób zakaźnych** (art. 9 ust. 2 lit i art. 6 ust. 1 lit d RODO). O legalności tych działań świadczy również motyw 46 RODO, zgodnie z którym przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest to niezbędne do ochrony interesu, które ma istotne znaczenie dla życia osoby której dane dotyczą np. gdy przetwarzanie jest potrzebne do celów humanitarnych w tym monitorowania epidemii i ich rozprzestrzeniania się.

Prezes UODO zachęca wszystkich zainteresowanych szczegółami realizacji działań związanych z walką z koronawirusem do kontaktu z GIS.

Źródło:

UODO: wysyłanie komunikatów dotyczących koronawirusa zgodne z RODO

Jak wyjaśnił Prezes UODO, przepisy RODO nie zabraniają przesyłania do użytkowników telefonów komórkowych wjeżdżających do Polski komunikatów dotyczących rozprzestrzeniania koronawirusa 2019-nCoV.

Przesyłanie komunikatów w wykonaniu ustawowego obowiązku.

Komunikat Prezesa UODO to odpowiedź na prośbę Ministra Cyfryzacji dotyczącą oceny planowanych działań dotyczących epidemii koronawirusa – czy działania te są zgodne z przepisami o ochronie danych osobowych. Oczywiście jest to podyktowane ostatnimi wydarzeniami związanymi z rozprzestrzenianiem się wirusa. Z tego względu rząd uznał za konieczne podjęcie pilnych działań polegających na informowaniu osób przybywających do Polski o działaniach, jakie zaleca się podjąć w przypadku podejrzenia zarażenia koronawirusem.

W ocenie Prezesa UODO zastosowanie w tym przypadku ma art. 21a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. W związku z tym na żądanie Rządowego Centrum Bezpieczeństwa **należy wysyłać komunikaty** o zagrożeniu wystąpieniem sytuacji kryzysowej przez operatorów sieci telekomunikacyjnej.

GPA publikuje stanowiska organów ochrony danych dotyczące koronawirusa

Global Privacy Assembly (światowa organizacja zrzeszająca rzeczników ochrony danych osobowych) uruchamia specjalną zakładkę na swojej stronie internetowej, w której zamieszczane są oświadczenia poszczególnych organów ochrony danych. Dotyczą one działań podejmowanych w walce z koronawirusem.

W zakładce zbierane będą informacje z poszczególnych państw – w postaci linków do stanowisk organów ds. ochrony danych osobowych dotyczących koronawirusa. Zakładka będzie więc kompendium wiedzy na temat praktyk z całego świata.

Zbiór stanowisk organów ochrony danych osobowych

Celem tego rozwiązania ma być wymiana wiedzy, doświadczeń i ekspertyz. Dzięki temu organy ochrony danych będą mogły lepiej wypełniać swoje obowiązki w tym trudnym okresie. **Ze wskazówek mogą również skorzystać administratorzy danych osobowych.**

Oświadczenie Komitetu Wykonawczego GPA znajdziesz tutaj>>. Natomiast oświadczenia poszczególnych organów ochrony danych dostępne są tutaj>>

Źródło:
Strona internetowa UODO (uodo.gov.pl)

Pracodawca i dane osobowe pracownika w czasie epidemii

W związku z rozszerzającą się epidemią COVID-19 wiele osób ma wątpliwości jakie dane pracowników pracodawca może przetwarzać i w jakim celu. W artykule przybliżymy tą tematykę, regulowaną nie tylko specustawą ale i ogólnymi przepisami ochrony danych osobowych.

Specustawa już działa

W dniu 2 marca 2020 roku Sejm przyjął ustawę o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych. Zgodnie z jej art. 37 wchodzi ona w życie w dzień po jej ogłoszeniu. Została ona ogłoszona 7 marca a więc weszła w życie 8 marca 2020 roku.

Ustawa dotyczy w zasadzie wszystkiego co związane z szerzącą się aktualnie epidemią tzw. koronawirusa (SARS-CoV-2, COVID-19): zwalczanie wirusa, działania przeciwepidemiczne i zapobiegawcze, obowiązki poszczególnych podmiotów oraz zasady finansowania tych działań. Ta specustawa nie wyłącza możliwości zastosowania instrumentów z ustawy systemowo regulującej kwestie chorób zakaźnych (tj. ustawy z dnia 5 grudnia 2008 roku o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi).

Zalecana praca zdalna

Pracodawcy zyskali możliwość polecenia pracownikowi wykonywania pracy zdalnej. Chodzi tu o wykonywanie pracy określonej w umowie o pracę, jednak poza miejscem jest stałego wykonywania. Pracodawca musi jednak określić przez jaki oznaczony czas taka praca zdalna ma być wykonywana a po drugie, wydanie polecenia musi mieć za cel przeciwdziałanie COVID-19.

Instrument ten pozwala pracodawcy na przetwarzanie danych osobowych pracownika w postaci informacji o tym czy pracownik przebywał ostatnio **na obszarze zagrożonym epidemią koronawirusa** (np. będąc na urlopie). Nie wydaje mi się przy tym czy zasadne jest pytanie o dokładny kierunek przyjazdu (np. Włochy czy Chiny), ważne jest to czy pracownik przebywał na obszarze o zwiększonym ryzyku zachorowania czy też w strefie wolnej od wirusa. W takim przypadku podstawą

przetwarzania danych osobowych będzie art. 6 ust. 1 lit. f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO), tj. prawnie uzasadniony interes administratora danych. Administrator danych (czyli pracodawca) ma bowiem interes w zapewnieniu bezpieczeństwa pracowników i innych osób przebywających na terenie zakładu pracy. I jest to interes prawnie uzasadniony chociażby z powodu możliwości wydania takiemu pracownikowi polecenia pracy zdalnej. Trudno również dopatrzyć się w takim zachowaniu pracodawcy jakiegoś naruszenia interesów lub podstawowych praw i wolności pracownika.

Po drugie, niemal zawsze będzie spełniona jednocześnie druga z przesłanek przetwarzania danych (z art. 6 ust. 1 lit. d RODO). Należy bowiem zauważyć, że skoro informacja o kierunku przyjazdu jest niezbędna do zapewnienia bezpieczeństwa pracowników lub innych osób przebywających na terenie zakładu to jednocześnie przetwarzanie tej informacji jest niezbędne dla ochrony żywotnych interesów innych osób fizycznych niż podmiot danych. Te żywotne interesy to bowiem nic innego jak życie i zdrowie, zagrożone przez COVID-19. Wprawdzie przesłanka ta, zgodnie z motywem 46 do RODO, dotyczy właśnie „celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się" ale ma jednocześnie charakter posiłkowy, rezerwowy względem innych przesłanek.

W przypadku kontroli Prezesa UODO należy się więc w pierwszej kolejności powołać na art. 6 ust. 1 lit. f RODO.

Zadanie nakazane czyli premier lub wojewoda każe pracodawcy

Premier na wniosek wojewody i po poinformowaniu ministra właściwego do spraw gospodarki może wydawać polecenia różnym osobom prawnym i jednostkom organizacyjnym nieposiadającym osobowości prawnej oraz przedsiębiorcom. Adresatem takiego zadania może być więc szeroko rozumiany pracodawca. Te polecenia:

- mają formę decyzji administracyjnej;
- podlegają natychmiastowemu wykonaniu z chwilą ich doręczenia lub ogłoszenia;
- nie wymagają uzasadnienia;
- mogą być wydawane ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej lub za pomocą innych środków łączności.

Wykonywanie zadań następuje na podstawie umowy zawartej z przedsiębiorcą przez właściwego wojewodę a jeśli przedsiębiorca nie zawrze umowy to zadanie wykonywane jest na podstawie samej decyzji. Podobne uprawnienia co do wydawania poleceń ma też wojewoda.

W takich przypadkach pracodawca będzie przetwarzał dane pracowników na podstawie art. 6 ust. 1 lit. c RODO, tj. takie przetwarzanie będzie niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Ten obowiązek będzie naturalnie wynikał z decyzji wojewody.

Badanie temperatury

Bez wątpienia jednorazowe zmierzenie temperatury nie jest przetwarzaniem danych wrażliwych (tj. danych o chorobie pracownika). Sam odczyt podwyższonej temperatury nie musi bowiem świadczyć o chorobie. Stan podgorączkowy też nie zawsze jest wynikiem choroby ale na przykład wzmożonego wysiłku fizycznego. Jest to więc jedynie informacja o chwilowym stanie jednego z parametrów określających fizyczny stan organizmu. W takim przypadku podstawy przetwarzania danych osobowych będą więc takie same jak przy kierunku urlopowym: art. 6 ust. 1 lit. d i f RODO.

Jeżeli zaś uznać taki pomiar za dane wrażliwe (np. gdy jest on dokonywany codziennie o tej samej porze albo temperatura jest tak wysoka że raczej wyklucza przyczynę inną niż choroba) to wówczas art. 9 ust. 2 lit. g RODO pozwala na przetwarzanie danych wrażliwych gdy:

- jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g RODO);
- jest niezbędne do celów profilaktyki zdrowotnej, do oceny zdolności pracownika do pracy, zapewnienia opieki zdrowotnej (art. 9 ust. 2 lit. h RODO);
- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi (art. 9 ust. 2 lit. i RODO).

Badanie na koronawirusa

Poddanie pracownika badaniu na obecność koronawirusa to już bez wątpienia **przetwarzanie danych wrażliwych**. Konieczne jest więc spełnienie, którejś z przesłanek z art. 9 ust. 2 RODO, które wskazaliśmy powyżej. Najbardziej trafną i często spełnioną wydaje się przesłanka z art. 9 ust. 2 lit. i RODO a więc ocena zdolności pracownika do pracy. Należy pamiętać, że przesłanki przetwarzania danych muszą być spełnione także przez podmiot medyczny zatrudniony przez pracodawcę do pobrania i zbadania próbki. Dane wrażliwe przetwarzane muszą być przez pracodawcę tak samo jak inne podobne dane, np. te z orzeczeń lekarskich dot. zdolności do pracy.

Bez zgód będzie lepiej

Jak więc widzimy, pracodawca nie potrzebuje pobrania zgody pracownika na najbardziej typowe przypadki przetwarzania danych osobowych w związku z epidemią. Tym samym pobieranie takiej zgody należy uznać wręcz za **błąd**. Organ nadzorczy wielokrotnie zwracał uwagę, że pobieranie zgody przy zaistnieniu innej przesłanki przetwarzania danych osobowych nie jest działaniem prawidłowym bowiem daje pracownikowi fałszywe poczucie przetwarzania jego danych osobowych na podstawie tej zgody – a co za tym idzie, fałszywe poczucie możliwości skutecznego podniesienia sprzeciwu. Ponadto pracownik może odmówić udzielenia zgody – i jak wówczas pracodawca „namówi" go do współpracy argumentując, że zachodzi inna przesłanka przetwarzania danych? Pracodawca byłby wówczas niewiarygodny.

Wskazane wyżej przesłanki odnoszą się nie tylko do pracowników ale także takich osób trzecich, jak klienci czy dostawcy.

Podstawa prawna:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE.L nr 119, str. 1) - art. 6, art. 9,
- Ustawa z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. 2020 poz. 374)
- Ustawa z 8 marca 1990 r. o samorządzie gminnym (tekst jedn.: Dz.U. z 2019 r. poz. 506) – art. 5a ust. 1.

4 wskazówki dla ADO – jak zadbać o dane osobowe w pracy zdalnej

W ostatnim czasie, z powodu zagrożenia epidemicznego spowodowanego pandemią koronawirusa, wiele organizacji przeszło na model pracy zdalnej. Dzięki temu pracownicy mogą realizować swoje obowiązki z domu, wykorzystując narzędzia komunikacji elektronicznej do kontaktu z pozostałymi członkami zespołu. Taki sposób pracy oczywiście jest uzasadniony obecna sytuacją na świecie, ale nie można przy tym zapominać o konieczności odpowiedniego zabezpieczania informacji przechowywanych przez pracowników na komputerach w domu oraz przesyłanych przez Internet.

Przepisy prawa, które nakazują zachowanie poufności danych albo wewnętrzne ustalenia dot. zachowania w tajemnicy niektórych informacji obowiązują bowiem nadal. Konieczne jest więc taka organizacja pracy i wybór narzędzi, aby pracownicy mogli pracować zdalnie przy zapewnieniu odpowiedniego poziomu bezpieczeństwa informacji. Jakie działania powinna podjąć organizacja aby zapewnić odpowiedni poziom bezpieczeństwa?

Wskaż osoby odpowiedzialne za bezpieczeństwo

Osoby zajmujące się **wsparciem informatycznym** pracowników na co dzień z reguły są wyznaczane także do pomocy osobom pracującym zdalnie. Kwestia bezpieczeństwa danych powinna zostać potraktowana przez nie priorytetowo. Stąd też to one będą odpowiedzialne za konfigurację środowisk i urządzeń, które umożliwią bezpieczną pracę zdalna, wydanie pracownikom sprzętu, a następnie bieżące wsparcie ich (zdalne) w działaniu.

Ważne

Każdy z pracowników powinien mieć świadomość, do kogo może się zwrócić z prośbą o bieżące wsparcie techniczne.

Z drugiej strony, to na dziale IT spoczywa również obowiązek przekazywania informacji dotyczących tego jak zachować bezpieczeństwo podczas pracy zdalnej.

Wybierz odpowiednie urządzenia

Praca na plikach z danymi, udostępnionymi przez pracodawcę, w tym wymiana tych plików pomiędzy poszczególnymi pracownikami, powinna odbywać się przy wykorzystaniu **służbowych laptopów** – oczywiście o ile jest to technicznie możliwe. Pozwala to na zachowanie obowiązujących w organizacji zasad dotyczących:

- wykorzystania systemów operacyjnych,
- aktualizacji oprogramowania,
- instalacji programów antywirusowych
- ograniczenia możliwości korzystania z aplikacji niezatwierdzonych przez administratora.

Ważne

Praca zdalna prowadzona przy wykorzystaniu prywatnych urządzeń powinna być dopuszczana jedynie wyjątkowo.

Zapewnij bezpieczeństwo wiadomości e-mail

Samo przesyłanie informacji za pomocą e-maila powinno odbywać się przy użyciu służbowej skrzynki pocztowej danego pracownika.

1. W miarę możliwości, korespondencja elektroniczna powinna być szyfrowana (np. przy wykorzystaniu rozwiązań PGP lub S/MIME).

2. Jeżeli do korespondencji są dołączane załączniki zawierające np. dane osobowe albo inne informacje poufne, to powinny one także być zaszyfrowane (nawet jeśli nie szyfrujemy samej wiadomości).
3. Klucz rozszyfrowujący należy przekazywać odbiorcy innym niż e-mail kanałem komunikacji – np. SMSem.

Wybierz bezpieczne narzędzia do pracy zdalnej

W związku z ostatnimi wydarzeniami, znacznie zwiększa się popularność narzędzi ułatwiających pracę zespołów na odległość, wymianę plików, zarządzanie projektami czy kontrolę bieżących efektów prac. Wybór takiego narzędzia nie może odbywać się jednak bez wzięcia pod uwagę kwestii bezpieczeństwa. Konieczne wiec jest zweryfikowanie tego gdzie będą przechowywane nasze dane, ze szczególnym uwzględnieniem tego, czy mogą być one przetransferowane poza państwa należące do Europejskiego Obszaru Gospodarczego. Warto również sprawdzić, jakie **zabezpieczenia wdrożył dostawca** takiego narzędzia – np. czy szyfruje dane przechowywane w jego ramach. Dodatkowo, akceptowane przez nas regulaminy powinny zawierać postanowienia dotyczące powierzenia przetwarzania danych osobowych.

Szczególna sytuacja, w której obecnie się znajdujemy, nie zwalnia administratora z obowiązku stosowania się do zasad bezpieczeństwa, w tym również tych, które dotyczą pracy zdalnej.

Organizacje, które już wcześniej pozwalały niektórym pracownikom na wykonywanie zadań poza biurem, mają tu ułatwione zadanie. Często wewnętrzne procedury dotyczące bezpieczeństwa IT posiadają uregulowania dot. korzystania z narzędzi informatycznych poza standardowym miejscem pracy. Te przedsiębiorstwa, które nie praktykowały dotąd takiego modelu pracy, muszą się szybko dostosować do nowego otoczenia.

Zobacz także: Praca zdalna – co z bezpieczeństwem danych

Podstawa prawna:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE.L nr 119, str. 1) - art. 24, art. 32.

UODO radzi, jak pracujący zdalnie powinien chronić dane osobowe

W związku z zagrożeniem koronawirusem pracodawcy mają możliwość polecenia pracownikom pracy zdalnej czyli poza stałym miejscem wykonywania pracy np. w domu. Urząd Ochrony Danych Osobowych radzi, jak zadbać o ochronę danych przetwarzanych przez pracowników poza siedzibą administratora. Rady te warto przekazać pracownikom.

Urządzenia i oprogramowanie	Korzystając z urządzeń służbowych i zainstalowanego na nich oprogramowania postępuj zgodnie z przyjętą przez administratora procedurą bezpieczeństwa.
	Nie instaluj oprogramowania niezgodnego z procedurą bezpieczeństwa.
	Zadbaj o aktualizację oprogramowania, w tym antywirusowego.
	Wydziel sobie odpowiednią przestrzeń do pracy, by osoby postronne nie miały możliwości dostępu do dokumentów, nad którymi pracujesz.
	Jeśli odchodzisz od stanowiska pracy, blokuj urządzenie, na którym pracujesz.
	Zabezpieczaj dostęp do komputera – stosuj silne hasła dostępu, wielopoziomowe uwierzytelnianie.
	Zadbaj o archiwizację danych.
Poczta elektroniczna	Przestrzegaj przyjętej przez administratora procedury bezpieczeństwa w zakresie korzystania ze służbowej poczty e-mail.
	W miarę możliwości używaj służbowych kont e-mail.

	Zadbaj o właściwe szyfrowanie treści wiadomości i załączników, jeśli pracujesz na prywatnym sprzęcie.
	Każdorazowo przed wysłaniem maila upewnij się, czy adresujesz go do właściwej osoby.
	Nie odbieraj wiadomości od nieznanych adresatów (a w szczególności załączników w tych wiadomościach).
Chmura	Chmury używaj tylko z zaufanego dostępu.
	Przestrzegaj procedur odnośnie logowania do chmury.

Źródło:
Strona internetowa UODO (uodo.gov.pl)

Stopka redakcyjna

Redaktor:	Michał Kowalski
ISBN:	978-83-269-9096-0
E-book nr:	2HH1022
Firma:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł, Nr rejestrowy BDO: 000008579
Copyright by:	Wiedza i Praktyka sp. z o.o. Warszawa 2019