Obserwuj nas na:

Nr 5/2020 (14)
Maj 2020

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

PRACODAWCA NIE MOŻE MIEĆ WGLĄDU W BADANIA LEKARSKIE PRACOWNIKA

Zgodnie z obowiązującymi przepisami prawa, pracodawca nie jest uprawniony do pozyskiwania od podmiotu leczniczego informacji o skorzystaniu przez jego pracownika z konkretnej usługi medycznej. Ma jedynie prawo do otrzymania wydawanego przez lekarza orzecznika zaświadczenia o braku przeciwwskazań lub o istnieniu przeciwwskazań zdrowotnych danego pracownika do pracy na określonym stanowisku.

Zasad tych należy przestrzegać także wówczas, gdy pracodawca zawarł z placówką medyczną umowę na świadczenie usług dla jego pracowników i pokrywa ich koszty.

Do zajęcia takiego stanowiska skłania zarówno analiza przepisów RODO, jak i krajowych przepisów szczególnych.

Informacje opisujące rodzaj usługi medycznej, z jakiej skorzystał pacjent, należy uznać za dane o stanie zdrowia, które zgodnie z RODO należą do szczególnych kategorii danych osobowych. Można je zatem przetwarzać po spełnieniu ściśle określonych warunków.

Co istotne, przepisy ustawy z dnia 24 czerwca 1996 r. Kodeks pracy (art. 22^1) ustanawiają zamknięty katalog danych pracownika, które mogą być przetwarzane przez pracodawcę.

Oznacza to, że pracodawca nie może przetwarzać danych, które wykraczają poza ten zakres. Wprawdzie pracodawca nie może dopuścić do pracy pracownika bez aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na określonym stanowisku w warunkach pracy opisanych w skierowaniu na badania lekarskie, lecz przepisy prawa pracy zezwalają tylko na wydanie pracodawcy zaświadczenia o braku przeciwwskazań lub też o przeciwwskazaniach zdrowotnych danego pracownika do pracy na określonym stanowisku. Tym samym niedopuszczalne jest przetwarzanie przez pracodawcę innych informacji na temat pracownika, a w szczególności danych dotyczących jego stanu zdrowia, ponieważ pracodawca nie jest do tego uprawniony.

Informacja o wykonanych wobec pracownika usługach medycznych, choćby taka, jak skorzystanie z usługi specjalistycznej, poradni czy usługi rehabilitacyjnej, która trafiałaby do pracodawcy, stanowiłaby przetwarzanie danych pracownika dotyczących jego zdrowia.

Zatem nawet wówczas, gdy pracodawca zawarł z placówką medyczną umowę na świadczenie usług dla jego pracowników i pokrywa ich koszty, to sposób rozliczenia wykonanych świadczeń medycznych związany z wystawieniem przez usługodawcę faktury nie może prowadzić do przetwarzania szczególnych kategorii danych (danych dotyczących zdrowia) w taki sposób, że do konkretnego pracownika będą przypisane badania i konsultacje, które zostały mu zlecone przez lekarza. Także imienny wykaz pracowników wraz z adnotacją o skorzystaniu choćby z danej usługi medycznej prowadziłby do obejścia przytoczonych przepisów.

Dodatkowo należy pamiętać, że osoby wykonujące usługi medyczne mają obowiązek zachowania tajemnicy lekarskiej (mowa o niej w art. 40 ustawy z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty). Przekazując informacje o pacjentach osobom trzecim, narażałyby się zatem na zarzut jej naruszenia.

SPRAWDZANIE TEMPERATURY W CELU ZAPOBIEGANIA ROZPRZESTRZENIANIA SIĘ COVID-19

W sytuacji kiedy będzie dokonywany np. pomiar temperatury ciała danej osoby, czy też będą gromadzone dane dotyczące jej stanu zdrowia, a następnie informacje te będą w szczególności utrwalane, przekazywane i gromadzone, wówczas będzie następowało przetwarzanie szczególnej kategorii danych osobowych.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych przepisy o ochronie danych osobowych nie sprzeciwiają się przetwarzaniu danych pracowników i gości w zakresie np. mierzenia temperatury czy wdrażania kwestionariusza z objawami chorobowymi. RODO w swoim art. 9 ust. 2 lit. i) wskazuje, że szczególne kategorie danych (dotyczące zdrowia) można przetwarzać, gdy jest to niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi, jeżeli wynika to z przepisów prawa.

Zgodnie z art. 17 tzw. specustawy ws. koronawirusa, Główny Inspektor Sanitarny posiada uprawnienia, aby oddziaływać na inne podmioty oraz na zmiany w obowiązujących przepisach, a także wskazywać na przyjmowanie właściwych rozwiązań.

W ocenie Prezesa art. 17 specustawy nie wyklucza możliwości wprowadzenia przez pracodawców, czy przedsiębiorców ww. rozwiązań mających na celu zwalczanie COVID-19. W związku z tym, jeżeli inspektor sanitarny uzna, że niezbędne jest przyjęcie rozwiązania w postaci mierzenia temperatury pracownikom i tzw. gościom wchodzącym na teren zakładu pracy czy też pozyskiwania od pracowników oświadczeń dotyczących ich stanu zdrowia, może skorzystać z właściwego dla niego środka prawnego, w efekcie czego na zakład pracy nałożony zostanie obowiązek w postaci decyzji o dokonywaniu pomiaru temperatury czy też zbieraniu oświadczeń pracowników dotyczących ich stanu zdrowia.

Więcej informacji na stronie internetowej pod linkiem: https://uodo.gov.pl/pl/138/1516

POLECENIE WOJEWODY JAKO PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH

Polecenie wydane przez wojewodę na podstawie tzw. specustawy może stanowić samoistną podstawę prawną dla przetwarzania danych osobowych przez podmioty i organy w tym poleceniu wymienione.

Wojewoda – na potrzeby zapobiegania, przeciwdziałania i zwalczania COVID-19 – może wydawać polecenia obowiązujące wszystkie organy administracji rządowej działające w województwie i państwowe osoby prawne, organy samorządu terytorialnego, samorządowe osoby prawne oraz samorządowe jednostki organizacyjne nieposiadające osobowości prawnej. Uprawnia go do tego art. 11 ust. 1 zdanie pierwsze i drugie ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (tzw. specustawy). Polecenia te podlegają natychmiastowemu wykonaniu.

Zatem jeśli wojewoda takie polecenie wydał, to jest to wystarczająca podstawa prawna do przetwarzania danych przez podmioty w nim wymienione.

W opinii organu ochrony danych osobowych, ze względu na specyficzny charakter poleceń wojewodów wydawanych na podstawie art. 11 ust. 1 specustawy, stanowią one samoistną podstawę prawną w rozumieniu art. 9 ust. 2 lit. g RODO.

Zatem przykładowo, jeśli takim poleceniem wojewoda zobligował organy Państwowej Inspekcji Sanitarnej, by po zakwalifikowaniu danej osoby do objęcia kwarantanną przekazywały o tym informację do lokalnego ośrodka pomocy społecznej dla weryfikacji, czy nie wymaga ona pomocy żywnościowej, to na tej podstawie ośrodek pomocy społecznej może wnioskować do właściwego organu Państwowej Inspekcji Sanitarnej o przekazanie mu danych osób zakwalifikowanych do kwarantanny. Natomiast organ ten powinien przekazać ośrodkowi pomocy społecznej dane osób odbywających kwarantannę na obszarze jego działania. Ośrodek pomocy społecznej nie może jednak, powołując się na polecenie wojewody, wnioskować o przekazanie takich danych przez podmiot, który w takim poleceniu nie został wymieniony.

RELACJE MIĘDZY KRAJOWĄ RADĄ RIO A OBSŁUGUJĄCYMI JĄ IZBAMI

W sytuacji gdy poszczególne regionalne izby obrachunkowe zapewniają obsługę organizacyjną i techniczną Krajowej Rady Regionalnych Izb Obrachunkowych (RIO), możliwe jest zastosowanie koncepcji współadministrowania.

Takiej odpowiedzi Prezes UODO udzielił na pytanie przewodniczącej Krajowej Rady RIO dotyczące dookreślenia relacji zachodzących między wymienionymi podmiotami w związku z przetwarzaniem danych osobowych.

Wskazał, że analiza przepisów ustawy z dnia 7 października 1992 r o regionalnych izbach obrachunkowych, w tym sposobu tworzenia Krajowej Rady RIO oraz jej zadań i zasad pracy przesądza o statusie Krajowej Rady RIO jako administratora w rozumieniu art. 4 pkt 7 RODO.

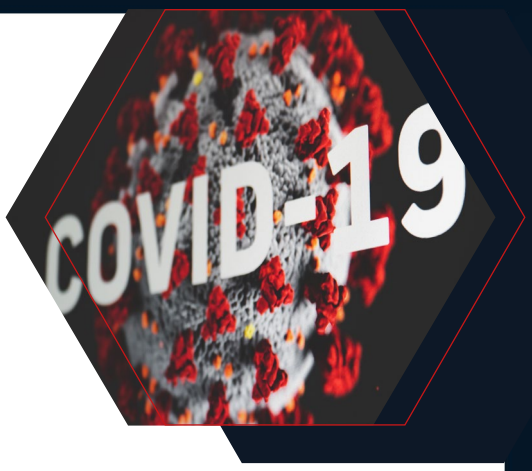
Natomiast w regulaminie Krajowej Rady RIO z 18 listopada 2009 r. określono (§ 18 i 19) niektóre zadania związane z obsługą Krajowej Rady Regionalnych Izb Obrachunkowych przez poszczególne regionalne izby, takie jak m.in. przyjmowanie i wysyłanie korespondencji, obsługę finansowo-księgową, przechowywanie dokumentacji.

Stwierdzić jednak należy, że zarówno przepisy ustawy o regionalnych izbach obrachunkowych, jak i regulaminu Krajowej Rady RIO nie przesądzają w pełni relacji zachodzącej między poszczególnymi regionalnymi izbami obrachunkowymi a Krajową Radą RIO. Można jednak zasadnie uznać, że w sytuacji, gdy regionalne izby obrachunkowe zapewniają obsługę organizacyjną i techniczną Krajowej Rady RIO, to w istocie wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Celowe jest zatem rozważenie zastosowania art. 26 RODO, czyli konstrukcji współadministrowania. Pozwoliłoby to im – w drodze wspólnych uzgodnień – w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w tym wskazać punkt kontaktowy dla osób, których dane dotyczą.

Należy jednak podkreślić, że zarówno Krajowa Rada RIO, jak i regionalne izby obrachunkowe mają swoje autonomiczne kompetencje. Zatem wspólnie powinny one uzgodnić inne kwestie, nieuregulowane wprost w przepisach prawa, w tym np. kwestię nadawania upoważnień do przetwarzania danych w ramach spraw prowadzonych przez Krajową Radę RIO, kwestię odpowiedniego zabezpieczenia danych osobowych, ochrony pomieszczeń czy też realizacji określonych obowiązków informacyjnych.

Dokonanie takich ustaleń umożliwiłoby doprecyzowanie sposobu obsługi technicznej Krajowej Rady RIO przez regionalne izby obrachunkowe przy zachowaniu autonomicznych kompetencji Krajowej Rady.

EROD



Wytyczne nt. przetwarzania danych w ramach walki z COVID-19 już są. Europejska Rada Ochrony Danych przyjęła wytyczne w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych, a także wytyczne odnoszące się do geolokalizacji i innych narzędzi ustalania kontaktów zakaźnych. Powstały one w związku z wybuchem pandemii COVID-19.

Decyzje w obu sprawach zapadły 21 kwietnia 2020 r. podczas 23. posiedzenia plenarnego Rady.

Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych objaśniają najpilniejsze kwestie prawne związane z wykorzystaniem danych odnoszących się do zdrowia, takie jak podstawa prawna przetwarzania, dalsze przetwarzanie danych dotyczących zdrowia do celów badań naukowych, wdrożenie odpowiednich zabezpieczeń i wykonywanie praw osób, których dane dotyczą.

EROD stwierdziła, że RODO zawiera kilka przepisów dotyczących przetwarzania danych na temat zdrowia do celów badań naukowych, które mają zastosowanie również w kontekście pandemii COVID-19, w szczególności w odniesieniu do zgody i odpowiednich przepisów krajowych. RODO przewiduje możliwość przetwarzania pewnych szczególnych kategorii danych osobowych, takich jak dane dotyczące zdrowia, gdy jest to konieczne do celów badań naukowych.

Ponadto wytyczne odnoszą się do kwestii prawnych związanych z międzynarodowym przekazywaniem danych dotyczących zdrowia do celów badań naukowych, związanych ze zwalczaniem pandemii COVID-19, w szczególności w przypadku braku decyzji stwierdzającej odpowiedni poziom ochrony lub innych odpowiednich zabezpieczeń.

Jednocześnie EROD pyrzjęła wytyczne 04/2020 dotyczące geolokalizacji i innych narzędzi ustalania kontaktów zakaźnych w kontekście wybuchu pandemii COVID-19. Te z kolei objaśniają warunki i zasady proporcjonalnego wykorzystania danych dotyczących lokalizacji i narzędzi ustalania kontaktów zakaźnych w dwóch konkretnych celach:

1) wykorzystanie danych dotyczących lokalizacji, aby wspierać reakcje na pandemię poprzez modelowanie rozprzestrzeniania się wirusa w celu oceny ogólnej skuteczności środków ograniczających jego rozprzestrzenianie się;

2) korzystanie z systemu ustalania kontaktów zakaźnych, by powiadomić osoby, które mogły znajdować się w bliskiej odległości od osoby, która ostatecznie została uznana za nosiciela wirusa, i w ten sposób jak najszybciej przerwać łańcuch zakażenia.

W wytycznych podkreślono, że zarówno RODO, jak i dyrektywa o prywatności i łączności elektronicznej zawierają szczegółowe przepisy pozwalające na wykorzystanie danych anonimowych lub osobowych w celu wsparcia władz publicznych i innych podmiotów zarówno na szczeblu krajowym, jak i unijnym, w ich wysiłkach na rzecz monitorowania i powstrzymania rozprzestrzeniania się COVID-19. Ogólne zasady skuteczności, konieczności i proporcjonalności muszą przyświecać wszelkim środkom przyjętym przez państwa członkowskie lub instytucje UE, które obejmują przetwarzanie danych osobowych w celu zwalczania COVID-19.

Ponadto EROD podtrzymuje stanowisko wyrażone w piśmie z 14 kwietnia 2020 r. do Komisji Europejskiej, że stosowanie aplikacji umożliwiających śledzenie kontaktów zakaźnych powinno być dobrowolne i nie powinno opierać się na śledzeniu przemieszczania się poszczególnych osób, lecz na informacjach o bliskości użytkowników.

Jak wyjaśniła Andrea Jelinek, przeowdnicząca EROD: Aplikacje nie zastąpią nigdy pielęgniarek i lekarzy. Chociaż dane i technologia mogą być ważnymi narzędziami, musimy pamiętać, że mają one wewnętrzne ograniczenia. Aplikacje mogą jedynie uzupełniać skuteczność środków ochrony zdrowia publicznego i zaangażowanie pracowników służby zdrowia, które jest niezbędne do walki z COVID-19. W żadnym razie ludzie nie powinni być zmuszeni do wyboru między skuteczną reakcją na kryzys a ochroną praw podstawowych.

Ponadto EROD przyjęła przewodnik dotyczący aplikacji do ustalania kontaktów zakaźnych jako załącznik do wytycznych. Celem tego przewodnika jest dostarczenie ogólnych wskazówek projektantom i osobom wdrażającym aplikacje umożliwiające ustalanie kontaktów zakaźnych, przy zaznaczeniu, że każda ocena musi być przeprowadzana indywidualnie dla każdego przypadku.

Decyzją EROD oba dokumenty wyjątkowo nie zostaną przedłożone do konsultacji społecznych ze względu na pilny charakter obecnej sytuacji i konieczność zapewnienia niezwłocznego dostępu do wytycznych.

Szczegółowe informacje na temat 23. posiedzenia plenarnego EROD, a także pozostałych kwietniowych posiedzeń (19. z 3.04., 20. z 7.04., 21. z 14.04., 22. z 17.04.) wraz z tłumaczeniami dokumentów, w tym wytycznych 3/2020 oraz pisma do KE, są dostępne pod linkiem: https://uodo.gov.pl/pl/p/posiedzenia-plenarne-erod

RADA EUROPY

Rekomendacja Rady Europy w sprawie wpływu systemów algorytmicznych na prawa człowieka

Komitet Ministrów Rady Europy przyjął rekomendację w sprawie wpływu systemów algorytmicznych na prawa człowieka, w których wzywa 47 państw członkowskich do rozważnego i ostrożnego podejścia do rozwoju i stosowania systemów algorytmicznych oraz do przyjęcia ustawodawstwa, polityk i praktyk, które w pełni szanują prawa człowieka.

Jeszcze na etapie przygotowań rekomendacji, Komitet Konsultacyjny ds. Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (tzw. Komitet T-PD), którego członkiem jest Urząd Ochrony Danych Osobowych, na posiedzeniu plenarnym w listopadzie 2019 r., przyjął opinię dotyczącą projektu rekomendacji, w której odwoływał się do Zmodernizowanej Konwencji 108.

Przyjęta przez Komitet Ministrów rekomendacja stanowi zestaw wytycznych wzywających rządy do zapewnienia, aby nie naruszały one dla własnego użytku praw człowieka poprzez rozwój lub zamawianie systemów algorytmicznych. Ponadto władze państwowe powinny ustanowić skuteczne i przewidywalne ramy prawne, regulacyjne i nadzorcze, które będą zapobiegać, wykrywać, zakazywać i zaradzać naruszeniom praw człowieka, niezależnie od tego, czy wynikają one ze strony podmiotów publicznych lub prywatnych.

W rekomendacji uznaje się ogromny potencjał procesów algorytmicznych w zakresie wspierania innowacji i rozwoju gospodarczego w wielu dziedzinach, w tym w komunikacji, edukacji, transporcie, zarządzaniu i systemach opieki zdrowotnej. W związku z obecną pandemią COVID-19 systemy algorytmiczne są wykorzystywane do prognozowania, diagnozowania i przeprowadzania badań nad szczepionkami i metodami leczenia. Coraz większa liczba państw dyskutuje nad ulepszaniem cyfrowych środków do śledzenia rozprzestrzeniania się wirusa, opierając się na algorytmach i automatyzacji.

Jednocześnie rekomendacja ostrzega przed poważnymi wyzwaniami dla praw człowieka związanymi z wykorzystywaniem systemów algorytmicznych, głównie dotyczącymi praw do uczciwego procesu, prywatności i ochrony danych, wolności myśli, sumienia i wyznania, wolności wypowiedzi i zgromadzeń, równego traktowania oraz praw gospodarczych i społecznych.

Link do rekomendacji KMRE: Recommendation on the human rights impacts of algorithmic systems

Link do opinii Komitetu T-PD: https://rm.coe.int/t-pd-2019-09-en-opinion-on-cdmsi-draft-recommendation-1-/168098f0f6

MIĘDZYNARODOWE

Działania informacyjne nt. ochrony danych osobowych i koronawirusa podjął polski organ nadzorczy, ale zrobiły to także organy innych państw członkowski UE. Przedstawiamy wybrane odpowiedzi na najczęściej zadawane pytania, których udzieliły organy nadzorcze z Finlandii, Francji i Szwecji.

FINLANDIA

Czy pacjent może powiedzieć bliskiej osobie, czy cierpi na koronawirusa?

Informacje o infekcji wirusowej lub narażeniu na wirusa wprowadzone do dokumentacji pacjenta podlegają przepisom o ochronie danych osobowych. Jeżeli służby zdrowia ujawniają takie informacje np. członkom rodziny pacjenta, stanowi to ujawnienie dokumentacji pacjenta stronom trzecim. Ujawnienie informacji o pacjencie jest możliwe na podstawie przewidzianej w sekcji 13 ustawy o statusie i prawach pacjentów (ustawa o pacjencie).

Informacje o pacjencie mogą być przekazywane stronie trzeciej za pisemną zgodą pacjenta. Jeżeli pacjent nie jest w stanie ocenić znaczenia wyrażonej zgody, informacje mogą zostać przekazane za pisemną zgodą jego przedstawiciela prawnego. Ponadto z powodu nieświadomości lub z jakiegokolwiek innego porównywalnego powodu, krewny lub inny bliski krewny leczonego pacjenta może zostać poinformowany o tożsamości pacjenta i stanie zdrowia, chyba że istnieją powody, by sądzić, że pacjent odmówi. Będzie to musiało zostać ocenione indywidualnie dla każdego przypadku.

Jeśli pacjent nie jest w stanie podjąć decyzji o leczeniu z powodu zaburzenia psychicznego, niepełnosprawności rozwojowej lub z innego powodu, przed podjęciem ważnej decyzji dotyczącej leczenia, aby ustalić, które leczenie najlepiej odpowiada woli pacjenta, należy skonsultować się z jego prawnym przedstawicielem, bliskim krewnym lub inną bliską osobą. W takim przypadku należy uzyskać zgodę tej osoby na leczenie. W takiej sytuacji przedstawiciel prawny pacjenta, bliski krewny lub inny bliski krewny ma prawo do uzyskania niezbędnych informacji o stanie zdrowia pacjenta w celu konsultacji i zgody.

Czy można powiedzieć rodzinie beneficjenta opieki społecznej, że cierpi on na koronawirusa?

Informacje o infekcji lub narażeniu na wirusa zapisane w danych beneficjentów opieki społecznej podlegają przepisom o ochronie danych. Jeśli takie informacje są przekazywane na przykład krewnemu beneficjenta jest to ujawnienie informacji o beneficjencie opieki społecznej. W takim przypadku należy przestrzegać sekcji 14–16 ustawy o statusie i prawach beneficjenta opieki społecznej (ustawa o beneficjencie pomocy społecznej).

Zgodnie z sekcją 16 ustawy o beneficjencie opieki społecznej informacje na temat dokumentu poufnego mogą być przekazywane za wyraźną zgodą beneficjenta lub zgodnie z odrębnym prawem. Jeżeli beneficjent nie jest w stanie ocenić znaczenia wyrażonej zgody, informacje można przekazać za zgodą jego przedstawiciela ustawowego.

Artykuł 9 ustawy o beneficjencie opieki społecznej przewiduje prawo do samostanowienia w szczególnych sytuacjach. W sytuacji, o której mowa w tej sekcji, wola beneficjenta musi zostać ustalona we współpracy z jego przedstawicielem ustawowym, krewnym lub inną osobą, gdy sam beneficjent nie jest w stanie uczestniczyć i wpływać na planowanie i wdrażanie swoich usług lub innych środków pomocy społecznej. Również w tym przypadku należy zauważyć, że nawet w szczególnej sytuacji wskazanej w tym prawie, informacje nie mogą zostać ujawnione krewnym, jeśli nie są wyraźnie związane z organizacją usług opieki społecznej dla indywidualnego beneficjenta. Ponadto zdolność klienta do podejmowania decyzji w tej sprawie musi zostać znacznie ograniczona, aby sekcja miała zastosowanie. Strona odpowiedzialna za usługi pomocy społecznej ustala, czy sytuacja klienta spełnia kryteria określone w sekcji 9 ustawy o beneficjencie pomocy społecznej.

Czy jednostka opieki zdrowotnej może kontaktować się z osobami w wieku powyżej 70. roku życia w ich okolicy i mapować ich stan zdrowia oraz potencjalne potrzeby pomocy?

Zdaniem EROD dane pacjenta można wykorzystać do mapowania, gdy można uznać to zadanie za część zadań jednostki opieki zdrowotnej, a celem jest ocena potrzeby opieki nad osobą.

Jeżeli w trakcie kontaktu osoba wyrazi chęć lub potrzebę skorzystania z usług świadczonych przez inne strony, informacje mogą zostać przekazane tym stronom za zgodą zainteresowanej osoby. W niektórych przypadkach przekazywanie informacji może być również zgodne z prawem.

Przetwarzanie danych osobowych związanych z mapowaniem należy zaplanować z wyprzedzeniem (uwzględnienie w fazie projektowania i domyślna ochrona danych zgodnie z art. 25 ogólnego rozporządzenia o ochronie danych). W szczególności należy zadbać o to, aby osoby zaangażowane w tworzenie map brały pod uwagę kwestie związane z poufnością oraz zasadę minimalizacji danych.

Czy podczas pandemii można wprowadzić nowe środki komunikacji w służbie zdrowia?

Służba zdrowia może tworzyć takie rozwiązania podczas pandemii. Pandemia nie jest jednak podstawą do nieprzestrzegania zasad ochrony danych, ale należy ją wziąć pod uwagę w wyjątkowych okolicznościach przy podejmowaniu decyzji o przetwarzaniu danych osobowych.

Wybrany instrument musi zwracać szczególną uwagę na bezpieczeństwo danych, aby zapobiec przekazywaniu danych osobom trzecim. Zgodnie z art. 32 ogólnego rozporządzenia o ochronie danych UE administrator i podmiot przetwarzający wdrażają środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku dla praw i wolności osób fizycznych.

Administrator musi ocenić, czy wprowadzenie nowego instrumentu powinno podlegać ocenie skutków zgodnie z art. 35 rozporządzenia o ochronie danych.

Podjęte środki i wprowadzone rozwiązania powinny być udokumentowane w celu realizowania zasady rozliczalności.

Źródło: https://tietosuoja.fi/en/coronavirus-covid-19

FRANCJA

Porady CNIL w zakresie wdrażania telepracy w kontekście COVID-19

Telepraca jest rozwiązaniem, któremu muszą towarzyszyć wzmocnione środki bezpieczeństwa w celu zagwarantowania bezpieczeństwa systemów informatycznych i przetwarzanych danych. CNIL publikuje zalecenia mające na celu pomoc w zabezpieczeniu danych osobowych podczas tego przejścia.

Zabezpiecz swój system informatyczny:

- Opublikuj kartę bezpieczeństwa telepracy lub w obecnym kontekście, przynajmniej zestaw minimalnych zasad, których należy przestrzegać, i przekaż ten dokument swoim pracownikom zgodnie z wewnętrznymi zasadami.

- W przypadku konieczności modyfikacji zasad zarządzania systemem informatycznym w celu umożliwienia telepracy (zmiana zasad autoryzacji, zdalny dostęp administratora itp.), należy oszacować związane z tym ryzyko i w razie potrzeby podjąć niezbędne działania.

- Wyposaż wszystkie stanowiska pracy swoich pracowników w co najmniej jeden firewall, program antywirusowy i narzędzie do blokowania dostępu do złośliwych witryn.

- Należy jak najszybciej utworzyć sieć VPN, aby uniknąć bezpośredniej ekspozycji usług w Internecie. W miarę możliwości należy włączyć dwustopniowe uwierzytelnianie VPN.

Jeśli twoje usługi są w Internecie:

- Zastosuj protokoły gwarantujące poufność i uwierzytelnienie serwera adresata, takie jak HTTPS dla stron internetowych i SFTP do przesyłania plików, korzystając z najnowszych wersji tych protokołów.

- Zastosuj najnowsze poprawki zabezpieczające do używanego sprzętu i oprogramowania (VPN, rozwiązanie zdalnego pulpitu, wiadomości, wideokonferencje itp.). Regularnie zapoznawaj się z biuletynem CERT-FR, aby otrzymać ostrzeżenie o najnowszych lukach w oprogramowaniu i dowiedzieć się, jak się przed nimi zabezpieczyć.

- Wdrażaj zastosowanie mechanizmów dwustopniowego uwierzytelniania w odniesieniu do zdalnie dostępnych usług w celu ograniczenia ryzyka włamania.

- Regularnie sprawdzaj dzienniki dostępu do zdalnie dostępnych usług pod kątem podejrzanych zachowań.

- Nie udostępniaj bezpośrednio niezabezpieczonych interfejsów serwera.

Ogólnie rzecz biorąc, należy ograniczyć liczbę dostępnych usług do ścisłego minimum, aby zmniejszyć ryzyko ataków.

Źródło: https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mettre-en-place-du-teletravail

SZWECJA
Nauczanie cyfrowe

Z powodu wybuchu koronawirusa wiele szkół, uczelni wyższych i uniwersytetów prowadzi kształcenie na odległość. Ogólne rozporządzenie o ochronie danych (RODO) nie stanowi przeszkody w edukacji on-line, ale ustanawia wymagania dotyczące ochrony interesów uczniów i nauczycieli.

Podmiot przetwarzający i administrator danych muszą opierać się na RODO. To osoba odpowiedzialna za dane osobowe musi między innymi zdecydować, w jaki sposób powinno odbywać się przetwarzanie i jakie dane osobowe są niezbędne, aby móc prowadzić nauczanie zdalne.

Kto jest odpowiedzialny za dane osobowe?

Odpowiedzialność za dane osobowe to czynność, która decyduje o tym, w jakim celu dane osobowe mają być przetwarzane i jak powinno odbywać się przetwarzanie.

Ważną częścią pracy administratora ochrony danych jest udzielenie uczniom i nauczycielom jasnych instrukcji, jak radzić sobie z nauczaniem cyfrowym. Ważnym punktem wyjścia jest to, że administrator danych nie powinien przetwarzać więcej danych osobowych, niż jest to konieczne do realizacji celów.

Podstawa prawna przetwarzania danych osobowych

Wszelkie przetwarzanie danych osobowych musi mieć podstawę prawną zgodnie z ogólnym rozporządzeniem o ochronie danych. Bez podstawy prawnej przetwarzanie danych osobowych jest niezgodne z prawem.

Ogólny interes publiczny jest podstawą prawną, która może być najczęściej wykorzystywana do przetwarzania danych osobowych zarówno w szkołach prywatnych, jak i publicznych. Przykładami przetwarzania danych osobowych, które są niezbędne do wykonania zadania leżącego w ogólnym interesie szkolnym, jest przetwarzanie danych osobowych w celu zapewnienia, organizacji i prowadzenia nauczania.

Należy pamiętać, że zgoda nie jest zwykle wykorzystywana jako podstawa prawna do przetwarzania danych osobowych w szkole. Wynika to ze znacznej nierówności w relacji między osobą, której dane dotyczą, a administratorem danych, to znaczy między uczniem a szkołą. Dotyczy to również relacji między pracownikami a pracodawcami, czyli nauczycielem i szkołą.

Poinformuj uczniów o tym, co ma zastosowanie

Uczniowie muszą zostać poinformowani o zasadach postępowania, które mają zastosowanie podczas nauczania, na przykład o tym, jak korzystać ze sprzętu szkolnego i o zasadach korzystania z prywatnego telefonu komórkowego podczas lekcji. To, co dotyczy zwykłego nauczania w szkole, powinno dotyczyć również nauczania cyfrowego.

Nie przetwarzaj więcej danych osobowych niż to konieczne

Ważne jest, aby pamiętać, że nie należy przetwarzać większej liczby danych osobowych, niż jest to konieczne do prowadzenia nauczania przez szkołę. Ponieważ dzieci wymagają szczególnej ochrony, należy rozważyć, czy konieczne jest rejestrowanie obrazu i dźwięku w nauczaniu on-line.

Administrator danych musi zastanowić się nad wieloma pytaniami:

- W jaki sposób dzieci powinny brać udział w nauczaniu, zachowując ochronę ich danych osobowych?

- W jaki sposób zapewni ochronę danych osobowych uczniów i nauczycieli przed nieupoważnionym dostępem?

- Czy nauczanie powinno być nagrywane czy transmitowane na żywo?

- Jakiego sprzętu należy użyć?

- W jaki sposób osoba odpowiedzialna za dane osobowe zapewnia, że dane osobowe uczniów i nauczycieli nie są rozpowszechniane?

Źródło: https://www.datainspektionen.se/vaglednin-gar/skolor-och-forskolor/digital-undervisning/

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych" w sekcji „Zadania IOD" została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Czy z dokumentacji pracowniczej należy usuwać dane nadmiarowe?
Jakie informacje o pracownikach można udostępnić jako informację publiczną?
Czy należy odbierać zgodę na przetwarzanie od osób będących na kwarantannie?
Czy w przypadku kierowania studenta na praktyki zawodowe konieczne jest powierzenie?

URZĄD OCHRONY DANYCH OSOBOWYCH