FUNDACJA IM. STEFANA BATOREGO

forumIdei

Instytucje samorządowe w okresie SARS CoV-2: praca zdalna i wsparcie społeczności lokalnej. Analiza prawna

Agnieszka Krzyżak, Paweł Litwiński

Zapobieganie rozprzestrzeniania się SARS CoV-2 wymusiło poszukiwanie nowych rozwiązań działania samorządów, dotyczących m.in. obiegu korespondencji w urzędach, organizacji pracy zdalnej oraz zapewnienia wsparcia społeczności lokalnej.

Najważniejsze wnioski wynikające z obecnej sytuacji:

- Zmiana systemu pracy urzędów nie warunkuje zmiany w podejściu do zagadnień bezpieczeństwa. W przypadku pracy zdalnej adekwatne pozostają zasady i środki zabezpieczające, które funkcjonują z powodzeniem wewnątrz instytucji.
- Reorganizacja trybu pracy może być dobrą sposobnością do weryfikacji, czy zastosowane środki zabezpieczające są wystarczające i skuteczne, oraz podstawą do ewentualnego uszczelnienia systemu bezpieczeństwa.
- Przy udostępnianiu danych należy uwzględniać podstawowe zasady przetwarzania danych, w tym zasady legalności i zasady ograniczenia celu przetwarzania.

Pogarszająca się sytuacja związana z rozprzestrzenianiem się zakażenia wirusem SARS CoV-2 wpłynęła na sposób funkcjonowania sektora publicznego na niespotykaną dotąd skalę. Niemal z dnia na dzień wiele urzędów i instytucji publicznych zamknięto, a realizacja obowiązków na nich spoczywających uległa reorganizacji.

Do tej pory dominującym miejscem pracy dla sektora publicznego były gmachy urzędów. Upowszechnienie w ostatnim czasie pracy zdalnej dotyka tego sektora na niespotykaną skalę. Wielu pracowników, nigdy dotąd nierealizujących obowiązków służbowych w trybie zdalnym, odesłano do pracy w domu. Zarówno kierujący instytucjami publicznymi, jak i szeregowi pracownicy stanęli przed wyzwaniem odpowiedniego i bezpiecznego zorganizowania pracy w nowych warunkach. Sytuacji na pewno nie pomaga wciąż słaba w porównaniu do sektora prywatnego, choć

sukcesywnie postępująca, informatyzacja instytucji publicznych. Przekierowanie komunikacji i zmiana trybu pracy są ogromnym wyzwaniem dla instytucji samorządowych[1].

Na instytucje publiczne nałożono również dodatkowe obowiązki związane ze świadczeniem pomocy społeczności lokalnej, która została dotknięta obostrzeniami wynikającymi z przeciwdziałania rozprzestrzenianiu się epidemii. Nie tylko obowiązek, ale i chęć wsparcia mieszkańców w tym trudnym czasie rodzą jednak wiele wątpliwości, w tym również dotyczących zapewnienia mieszkańcom prywatności.

Obieg korespondencji i dokumentacji wewnętrznej w instytucji

W związku z dużą odpornością wirusa na warunki środowiskowe panujące poza ludzkim organizmem oraz w nawiązaniu do informacji przekazywanych przez Światową Organizację Zdrowia (World Health Organization, WHO) i Centers for Disease Control and Prevention (CDC) wiele instytucji, nie tylko publicznych, nie przyjmuje poczty w wersji tradycyjnej (papierowej) lub wprowadziło szczególne obostrzenia związane z korespondencją przychodzącą i sposobem jej podejmowania oraz dalszej dystrybucji. Zgodnie z nowymi zasadami korespondencja przychodząca jest pozostawiana bez dalszego procedowania przez dwa, a czasem nawet cztery dni od dnia wpływu. Dopiero po tym czasie listy są otwierane i dystrybuowane dalej, do konkretnych wydziałów.

Z jednej strony, postępowanie takie jest uzasadnione względami bezpieczeństwa. Jak potwierdza CDC, wirus SARS CoV-2 potrafi przetrwać na powierzchniach nieożywionych, takich jak metal, szkło, plastik, nawet przez 17 dni[2]. Z drugiej strony, paraliż korespondencji przychodzącej na ponad dwa tygodnie od daty jej wpływu powoduje poważne opóźnienia w działaniu, co jest szczególnie istotne w przypadku instytucji publicznych. Należy również zwrócić uwagę, że pozostawienie korespondencji przychodzącej w swego rodzaju „kwarantannie" przez okres nieprzekraczający czasu wskazywanego przez CDC nie będzie skuteczne[3]. Trzeba zatem opracować mechanizmy, które z jednej strony pozwolą na sprawne i skuteczne funkcjonowanie instytucji, z drugiej zaś zminimalizują lub wyeliminują ryzyko związane z przenoszeniem wirusa SARS CoV-2 na powierzchni dystrybuowanej korespondencji.

Pomocna może okazać się dezynfekcja odbieranych przesyłek pocztowych, przy czym może ona wpływać negatywnie na stan listów (wiele środków dezynfekujących może uszkadzać złej jakości wydruki, trzeba również zwrócić uwagę na to, że oryginałów pism urzędowych nie wolno narażać na zniszczenie). Alternatywą może być np. nakaz odbierania poczty w rękawiczkach i podpisywania odbioru listów poleconych własnym długopisem. W kwestii dalszej dystrybucji korespondencji zaleca się rozważenie wprowadzenia obowiązku skanowania listów i ich przekazywania dalej wyłącznie w formie elektronicznej. W ten sposób do minimum byłby ograniczony kontakt fizyczny z nośnikiem papierowym, na którym może być przenoszony patogen. Dobór środków należy jednak do osoby decydującej o organizacji pracy w danej jednostce.

1 Opinia została opracowana na podstawie przepisów prawa powszechnie obowiązującego, w szczególności 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 osobowych, dalej jako: r.o.d.o.).

2 https://www.cdc.gov/mmwr/volumes/69/wr/mm6912e3.htm, dostęp: 10 kwietnia 2020.

3 Warto podkreślić, że niektóre badania wskazują, że wirus nie jest zdolny do życia po 24 godzinach na kartonie: https://www.nejm.org/doi/10.1056/NEJMc2004973 (przyp. red.).

Należy zatem w sposób racjonalny podchodzić do środków ostrożności, których celem jest przeciwdziałanie rozprzestrzenianiu się koronawirusa SARS CoV-2. Przede wszystkim, mając na względzie zdrowie i życie ludzi, pracodawca czy kierownik jednostki powinien wprowadzić odpowiednie systemowe środki bezpieczeństwa, które będą zarówno odpowiadały potrzebom związanym z przeciwdziałaniem zakażeniu, jak również będą funkcjonalne. W obecnej sytuacji epidemicznej rekomenduje się wprowadzenie formalnych procedur i instrukcji postępowania, w tym również z korespondencją przychodzącą. Wdrożenie takich procedur może odbywać się poprzez wyznaczenie osób odpowiedzialnych za realizację wskazanych obowiązków oraz zapoznanie wszystkich pracowników z nowymi warunkami pracy.

Akademia Samorządowa jest prowadzona przez Fundację im. Stefana Batorego i Stowarzyszenie POLITES. Skupia osoby od lat aktywne społecznie, m.in. biorące udział w akcji **Masz Głos**, które w wyborach samorządowych w 2018 roku weszły do władz lokalnych. Dziś są radnymi, sołtysami, wójtami i burmistrzami miast. W ramach **Akademii** zdobywają wiedzę, narzędzia, materiały i wsparcie eksperckie z zakresu najnowszych zmian w prawie samorządowym i dobrych praktyk samorządowca, a także poszerzają wiedzę o przepisach, procedurach, marketingu politycznym i przysługujących im uprawnieniach.

Analiza powstała z inspiracji uczestników Akademii, którzy zwrócili uwagę na konieczność wyjaśnienia kwestii związanych z pracą zdalną samorządów i wsparciem społeczności lokalnej w okresie epidemii.

Praca zdalna

Dokumentacja papierowa wynoszona z urzędów

Delegowanie pracowników do pracy zdalnej wymusza swego rodzaju przeniesienie biura na zewnątrz organizacji, poza ustalony dotychczas obszar przetwarzania danych. Oznacza to m.in. konieczność wyniesienia z zabezpieczonego obszaru przetwarzania dokumentów i nośników zawierających informacje o charakterze poufnym, w tym dane osobowe. Tym samym pojawia się ryzyko zagubienia, zniszczenia lub kradzieży dokumentów. Im dokument ważniejszy, tym wyższe ryzyko dla organizacji będzie stwarzała jego utrata. Aktywa w formie dokumentów trzeba więc należycie zabezpieczyć podczas wynoszenia poza ustalony i zabezpieczony obszar przetwarzania.

Duża odpowiedzialność w tym zakresie spoczywa na samym pracowniku. Wynoszone poza urząd czy instytucję dokumenty muszą pozostawać pod stałym nadzorem, co uniemożliwi ich przejęcie, zagubienie lub zapoznanie się z ich treścią przez osoby postronne, nieuprawnione do przetwarzania danych w organizacji. Szczególną ostrożność należy zachować przy transporcie poufnej dokumentacji. Nie powinna ona być pozostawiana bez nadzoru, otwierana publicznie bądź przekazywana osobom nieuprawnionym. Wysokim, choć niedocenianym, zagrożeniem jest ryzyko zapoznania się z treścią dokumentacji przez osoby trzecie, jeśliby była czytana w miejscu publicznym, np. podczas jazdy autobusem. Wynosząc dokumenty z organizacji, należy przez cały czas z należytą starannością dbać o ich poufność.

Warto zweryfikować szczelność systemu bezpieczeństwa i skuteczność stosowanych środków zabezpieczających, szczególnie środków organizacyjnych, które zapewniają poufność i chronią informacje, w tym dane osobowe. Kluczowe są odpowiedzi na pytania: czy pracownik wie, w jaki sposób postępować z dokumentacją w miejscu publicznym? Czy ma świadomość, jakie będą konsekwencje ujawnienia informacji, które przenosi? Czy wie, jak zabezpieczyć dokumenty poza obszarem, w którym w normalnych warunkach powinny się znajdować? Odpowiedzialność za zapewnienie poufności informacji

zawartych w dokumentach tradycyjnych spoczywa zatem w dużej mierze na kierowniku jednostki. Musi on zidentyfikować zagrożenia, przeciwdziałać zdarzeniom o negatywnym wpływie na informacje lub dane osobowe. Wskazane może okazać się przypomnienie pracownikom zasad postępowania z informacjami poufnymi, w tym z danymi osobowymi, oraz konsekwencji naruszeń ochrony danych. Należy również pamiętać, że naruszenie to nie tylko ujawnienie (naruszenie poufności), ale również zdekompletowanie lub nieuprawniona modyfikacja informacji. Być może konieczne będzie wprowadzenie dodatkowych, nowych środków zabezpieczających, szczególnie organizacyjnych, ale ta decyzja zależy od tego, jak zbudowany jest system bezpieczeństwa w konkretnej organizacji.

Ważną kwestią jest transport dokumentów z powrotem do instytucji. Jeśli dokument pozostawał poza urzędem przez dłuższy lub krótszy czas, mógł się stać medium dla przenoszenia wirusa SARS CoV-2, tak samo jak korespondencja przychodząca. W chwili sporządzania niniejszej opinii nie ma skutecznej rady, jak uniknąć tego zagrożenia. Wskazane może być zatem, aby systemowo wprowadzić zasadę, że wynoszenie dokumentów z organizacji jest ostatecznością, gdy niemożliwe jest np. ich zeskanowanie i transmisja w formie elektronicznej.

Korzystanie z prywatnych nośników pamięci

Nie wszystkie informacje przetwarzane są w formie papierowej. Dokumenty w formie elektronicznej, z uwagi na zmianę trybu pracy, w określonych warunkach muszą być przenoszone i przesyłane. Szczególnie przy wprowadzeniu wymogów skanowania korespondencji, transmisja i jej odpowiednie zabezpieczenie zyskują kluczowe znaczenie. Niestety, wiele instytucji nie dysponuje zewnętrznymi nośnikami pamięci masowej (np. pendrive) czy też posiada niewystarczającą liczbę takich nośników, stąd wielu pracowników będzie musiało posiłkować się sprzętem prywatnym. Należy przy tym pamiętać o paru zasadach, które pozwolą na uniknięcie luki w systemie bezpieczeństwa.

Najważniejsze, aby pracownik miał świadomość, że wymogi i regulacje dotyczące środków technicznych i organizacyjnych w zakresie zabezpieczenia sprzętu, na którym przetwarzane są dane osobowe, nie mogą być ograniczane do sprzętu służbowego. Poufność danych i informacji musi być chroniona całościowo. Wykorzystywanie prywatnego sprzętu do realizacji obowiązków służbowych nie powinno być podstawą dla wyjątków przy stosowaniu środków zabezpieczających przyjętych w danej instytucji. Zasadą powinno być więc, aby sprzęt prywatny, na którym pracownik ma wykonywać obowiązki służbowe, spełniał przynajmniej minimalne wymogi bezpieczeństwa i poufności przyjęte w danej organizacji. Jeżeli w danej instytucji nigdy nie określono progu minimum dla środków technicznych wykorzystywanych przy zabezpieczaniu informacji, reorganizacja pracy i oddelegowanie pracowników do pracy zdalnej może być dobrą okazją do ustalenia takich ram bezpieczeństwa.

W tym miejscu istotne jest również, by rozumienia pojęć „sprzęt" czy „urządzenie" nie ograniczać do komputera stacjonarnego lub laptopa, są to bowiem wszelkiego typu nośniki pamięci masowych, w tym zewnętrzne (zatem nie tylko dysk komputera przenośnego, ale także optyczne nośniki pamięci, pendrive'y), a także telefony komórkowe oraz tablety, które mogą służyć zarówno do realizacji obowiązków służbowych, jak też do transmisji informacji. Współczesne nośniki są niewielkie, co zwiększa ryzyko ich zagubienia. „Utrata urządzeń czy zewnętrznych nośników pamięci masowej może być bardzo niebezpieczna dla organizacji, a z uwagi na wymuszoną mobilność urządzeń i nośników, na których dane osobowe są zapisywane, ryzyko takiej utraty wzrasta"[4]. Ryzyko związane z zagubieniem

4 A. Krzyżak, A. Leńczuk, P. Barta, P. Litwiński, P. Licznar, *Koronawirus a prawo – prawo ochrony danych osobowych*, LinkedIn; https://www.linkedin.com/posts/barta-litwinski_koronawirus-a-prawo-prawo-ochrony-danych-activity-6652854606344835072-flKu?fbclid=IwAR0wMZ1kb3yUE4ePbBmd9_-gaF-qVyfztxaWHQP_JlOSXXZ7Xua_eZTTP2M, dostęp: 10 kwietnia 2020.

nośnika, w zależności od informacji przechowywanych na nośniku, może być bardzo wysokie (czego dowodem są np. przypadek SGGW[5] czy też naruszenie ochrony danych osobowych, jakie miało miejsce w Sądzie Okręgowym w Łodzi[6]).

Niedocenianym, lecz stosunkowo prostym środkiem zabezpieczającym transmisję danych w formie elektronicznej, jest szyfrowanie nośników i informacji na nich zapisanych. Oprogramowania szyfrujące są obecnie intuicyjne i powszechne, dostępne również w wersjach darmowych. Korzystanie z nich jest proste i często nie potrzeba specjalnego wykształcenia lub umiejętności, aby przeprowadzić szyfrowanie nośnika (jednak aby uniknąć kłopotów z odszyfrowaniem zabezpieczonego nośnika, warto poprosić o pomoc osobę posiadającą wiedzę z zakresu IT). Szyfrowanie skutecznie obniża prawdopodobieństwo wystąpienia negatywnych konsekwencji zagubienia lub utraty nośnika. Jeżeli w instytucji nigdy wcześniej nie stosowano tego środka zabezpieczającego, wskazane jest wdrożenie takiego rozwiązania z uwagi na zwiększoną transmisję informacji, w tym danych osobowych, w formie elektronicznej.

Należy również pamiętać o tym, że mimo wykorzystywania prywatnych nośników do transmisji okres retencji dla informacji i danych osobowych pozostaje niezmienny. Informacje zapisane na nośnikach prywatnych powinny być usuwane, zgodnie z przyjętymi politykami retencji, po upływie okresu przydatności przewidzianego dla danej informacji lub dokumentu.

Kolejną istotną kwestią jest zarządzanie nośnikami elektronicznymi wykorzystywanymi do transmisji i kontrola nad nimi. Pracodawca, kierownik jednostki czy też administrator danych powinni mieć możliwość nadzorowania, jakie medium jest wykorzystywane do przetwarzania informacji i danych osobowych. Taki organizacyjny środek zabezpieczający może obejmować np. obowiązek uzyskania pozwolenia na wykorzystanie nośnika prywatnego do celów służbowych oraz ewidencjonowanie nośników prywatnych wykorzystywanych w pracy. Rozwiązania w tym zakresie powinny być wprowadzone systemowo, w formie procedury lub instrukcji. Wypracowane zasady można wdrożyć jako element funkcjonującego w organizacji systemu bezpieczeństwa nawet po ustaniu stanu epidemii i po powrocie do normalnego trybu pracy.

Użytkowanie prywatnych komputerów do celów służbowych. Zabezpieczenia i problemy prawne

Ze względu na zmianę trybu wykonywania pracy na zdalny wielu pracowników musi posiłkować się własnym komputerem. Sprzęt ten pozostaje poza kontrolą pracodawcy, a jego oprogramowanie i parametry często znacznie różnią się od komputerów wykorzystywanych w organizacji.

Jeśli do celów służbowych wykorzystywany jest sprzęt prywatny, zarówno pracownik, jak i pracodawca muszą pamiętać o podstawowych zasadach. Ważne, aby urządzenie prywatne, na którym pracownik realizuje obowiązki służbowe, spełniało minimalne wymogi. Wypełnienie tych warunków stanowi wyzwanie nie tylko dla pracownika, ale również dla pracodawcy. W szczególności sprzęt wykorzystywany przez pracownika musi spełniać zarówno techniczne, jak i konfiguracyjne wymogi bezpieczeństwa stawiane w organizacji. Jak już zaznaczono, użycie prywatnego sprzętu nie może stanowić podstawy do ustalenia wyjątków w obowiązujących warunkach zabezpieczeń.

5 Szerzej: https://www.sggw.pl/aktualnosci/komunikat-o-naruszeniu-danych-osobowych, dostęp: 22 marca 2020.
6 Szerzej: https://lodz.so.gov.pl/informacja-dotyczaca-naruszenia-ochrony-danych-osobowych,new,mg,3,188.html,1085, dostęp: 10 kwietnia 2020.

Wśród najważniejszych środków zapewniających bezpieczeństwo sprzętów należy wymienić: aktualność oprogramowania, w tym aktualne i dobrze skonfigurowane oprogramowanie antywirusowe. Jak zaznaczał Prezes Urzędu Ochrony Danych Osobowych (PUODO): praca „na aktualnym systemie operacyjnym jest o tyle istotna, że niektóre z poprawek nie dotyczą wyłącznie kwestii bezpieczeństwa tego oprogramowania, ale również «załatania» luk wykrytych w konstrukcji podzespołów komputerowych. Istnieją rozwiązania, które z uwagi na błędy np. w procesorach naszych komputerów, pozwalają przejąć kontrolę nad całą maszyną (...) Dlatego, z punktu widzenia bezpieczeństwa danych osobowych, tak ważne jest korzystanie z aktualnego oprogramowania, zarówno komercyjnego, jak i tego, które można używać na licencji *open source*"[7]. Aktualizacje oprogramowania są zatem odpowiedzią na wszelkiego rodzaju luki bezpieczeństwa, w tym również nieprawidłowości w działaniu konkretnego sprzętu. Oprogramowanie antywirusowe broni przed zagrożeniem intencjonalnym, takim jak oprogramowania szpiegowskie, *malware* czy pozornie niegroźne „robaki" komputerowe. Te techniczne środki zabezpieczające powinny stanowić fundamentalne wymagania dla wszystkich sprzętów, niezależnie od tego, czy chodzi o urządzenie służbowe, czy też prywatny sprzęt wykorzystywany przez pracownika do celów służbowych. Jednocześnie nie są to wymogi wygórowane, zatem stawianie ich wobec prywatnych urządzeń pracownika nie uniemożliwia wykonywania przez niego pracy.

Wśród organizacyjnych środków zabezpieczających warto zwrócić uwagę na apel PUODO wystosowany w związku z zasadami bezpiecznej organizacji pracy zdalnej: „Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji"[8]. W przypadku korzystania przez pracowników z urządzeń prywatnych, zakaz podejmowania działań w celach osobistych może okazać się niemożliwy do wyegzekwowania. Stawianie takich wymagań będzie zatem ryzykowne dla całego systemu bezpieczeństwa informacji. Skoro jeden z warunków może być naruszany bez konsekwencji i nie ma możliwości jego egzekwowania, tak samo będą traktowane pozostałe zasady. „Niemniej wysoce wskazanym jest zwrócenie uwagi na to, by na sprzęcie służbowym lub wykorzystywanym w celach służbowych powstrzymać się od instalacji oprogramowania niezwiązanego z realizacją pracy i od aktywności prywatnej, w szczególności w trakcie połączenia zdalnego z systemami i zasobami administratora"[9].

Praca w domu nie zwalnia z obowiązku stosowania haseł oraz wygaszaczy ekranu. Adekwatne zastosowanie będą miały wszelkiego typu rygory związane z zawieszeniem lub zakończeniem pracy w systemie informatycznym. Mimo zmiany środowiska pracy, poufność informacji i danych jest nadal objęta ochroną, a pracownik nie został zwolniony ze stosowania się do wewnętrznych procedur i instrukcji postępowania.

W przypadku korzystania przez pracowników z komputerów prywatnych do realizacji obowiązków służbowych problematyczna może okazać się nie tyle kwestia zabezpieczenia tych urządzeń, co legalności korzystania z nich właśnie w takich celach. W szczególności dotyczyć to będzie oprogramowania komputerowego. Powszechnie wykorzystywany pakiet programów Microsoft Office występuje w wielu wersjach, zróżnicowanych w zależności od typu licencji udzielonej przez producenta.

Licencje tzw. komercyjne, a więc pozwalające na wykorzystywanie oprogramowania w celach zawodowych, są droższe, stąd z reguły wykupując pakiet do użytku domowego, użytkownik wybiera licencje o większych rygorach w kontekście pól eksploatacji, ale o niższej cenie. W konsekwencji wielu

7 https://uodo.gov.pl/pl/138/1359, dostęp: 22 marca 2020.
8 https://uodo.gov.pl/pl/138/1459, dostęp: 22 marca 2020.
9 A. Krzyżak, A. Leńczuk, P. Barta, P. Litwiński, P. Licznar, *Koronawirus a prawo...*, dz. cyt.

pracowników na prywatnych sprzętach ma zainstalowaną wersję nieprzeznaczoną do pracy w rozumieniu realizacji obowiązków służbowych. Wykorzystanie oprogramowania niekomercyjnego do celów zawodowych stanowi naruszenie warunków licencji, co w zależności od oprogramowania i umowy licencyjnej może w konsekwencji narażać użytkownika na odpowiedzialność cywilną lub nawet karną.

Naruszenia warunków licencji dokonuje osoba, która jest licencjobiorcą, w tym przypadku pracownik. Nie można jednak zapominać, że w związku z brzmieniem przepisów prawa pracy w przypadku wykorzystywania sprzętu prywatnego do wykonywania obowiązków służbowych to pracodawca zawiera z pracownikiem umowę, na podstawie której takie wykorzystywanie jest możliwe (art. 300 ustawy z dnia 26 czerwca 1974 r., Kodeks pracy, Dz. U. z 2019 r., poz. 1040; w zw. z art. 3531 i art. 60 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny, Dz. U. z 2019 r., poz. 1145). Zatem jeśli do złamania licencji dochodzi ze względu na polecenia wydawane przez pracodawcę, na urząd również może spaść odpowiedzialność za wykorzystywanie oprogramowania przez pracownika niezgodnie z warunkami licencji. Warto zwrócić uwagę, że pracownik występuje w podwójnej roli: jest zarówno licencjobiorcą oprogramowania, jak również podmiotem reprezentującym instytucję. Naruszenia dokonuje więc zarówno w imieniu własnym, jak i podmiotu, który reprezentuje.

Organizacja stanowiska pracy w miejscu zamieszkania oraz problem osób postronnych

Niezależnie od miejsca wykonywania pracy, informacje o charakterze poufnym, w tym dane osobowe, muszą pozostać zabezpieczone przed dostępem osób nieupoważnionych. Zapewnienie poufności informacji jest szczególnie trudne w przypadku pracy zdalnej wykonywanej w warunkach domowych. „Praca w warunkach domowych może stwarzać pozory bezpiecznej – przecież nikt niepożądany nie przejmie urządzenia w naszym własnym domu. Należy jednak pamiętać, że córka, syn, małżonek czy współlokator to również osoby nieupoważnione do przetwarzania danych osobowych, ergo nie powinni mieć dostępu do sprzętu i dokumentów, którymi posługuje się pracownik, oraz do informacji, jakie są w nich zapisane”[10]. Pojawia się zatem problem, jak pogodzić obowiązek zapewnienia poufności informacji i danych z wykonywaniem pracy w domu, gdzie środowisko pracy diametralnie różni się od codziennej rzeczywistości w urzędzie.

Kwestią priorytetową staje się konieczność organizacji środowiska pracy w domu. Podczas wykonywania obowiązków służbowych w warunkach domowych nie należy zapominać o podstawowych zasadach bezpieczeństwa i higieny pracy. Miejsce realizacji obowiązków nie ma wpływu na stosowanie zasad BHP. Pracownicy stają więc przed wyzwaniem – w swoich domach muszą zorganizować przestrzeń bezpieczną, pozwalającą na sumienną realizację obowiązków służbowych. Z jednej strony, zachowanie zasad BHP będzie miało znaczenie utylitarne. Wysoce niewskazane jest narażanie dokumentów na zalanie czy zniszczenie, dlatego nie powinno się jednocześnie gotować obiadu i czytać dokumentów. Z drugiej strony, dla ochrony zdrowia psychicznego samego pracownika praca zdalna nie powinna zdominować życia rodzinnego i naruszać miru domowego. Istotne staje się więc wyznaczenie granicy między pracą a życiem prywatnym.

W konsekwencji pracownik podejmujący pracę w formie zdalnej powinien wyznaczyć i zorganizować miejsce, gdzie będzie wykonywał obowiązki służbowe. Najlepiej, aby była to przestrzeń spokojna, niekoniecznie fizycznie wydzielona, jednak taka, która pozwoli na skupienie uwagi i ograniczy charakterystyczne dla warunków domowych rozluźnienie. Istotne jest poinformowanie pozostałych

10 Tamże.

domowników, że nawet pozostając w domu, pracujemy. Jeżeli realizujemy obowiązki służbowe, powinniśmy pamiętać o tym, że w przeciwieństwie do biura czy urzędu, w domu świadkami naszych słów i wykonywanych czynności mogą być osoby postronne. Osiągnięcie równowagi między środowiskiem domowym a wymogami stawianymi miejscu pracy może być szczególnie trudne w mieszkaniach, gdzie są dzieci lub przebywa dużo osób. Niemniej przejrzysta komunikacja z pozostałymi domownikami może przynieść niespodziewane efekty.

Kolejnym istotnym elementem jest zabezpieczenie sprzętu, na którym pracownik wykonuje obowiązki służbowe, oraz dokumentów i nośników informacji. Aktualne pozostają obowiązki wynikające z wewnętrznych regulacji pracodawcy, w tym obowiązki stosowania haseł i wygaszaczy ekranów. Opuszczając stanowisko pracy lub zawieszając wykonywanie obowiązków służbowych, należy zwrócić szczególną uwagę na to, czy wylogowaliśmy się z systemu informatycznego lub wirtualnej sieci prywatnej (VPN), czy zabezpieczyliśmy komputer (wylogowanie z systemu operacyjnego, wygaszacz ekranu), czy zamknęliśmy dokumenty w teczkach lub choćby usunęliśmy je z przestrzeni widocznej dla oka (np. poprzez schowanie w szufladzie).

Biorąc pod uwagę fakt, że pozostali domownicy w rozumieniu prawa ochrony danych są osobami nieupoważnionymi, należy ze szczególną uwagą podchodzić do możliwości naruszenia ochrony danych osobowych. Pracownikom podejmującym pracę zdalną należy przypomnieć, że „naruszenie ochrony danych lub incydent bezpieczeństwa, który ma miejsce podczas wykonywania pracy w formie zdalnej, wciąż jest takim samym incydentem lub naruszeniem jak w normalnych warunkach pracy. Pomimo zmiany trybu realizacji obowiązków służbowych, wdrożone procedury raportowania incydentów bezpieczeństwa i naruszeń mają zastosowanie również w odniesieniu do świadczenia pracy w formie zdalnej”[11].

Inicjatywy na rzecz społeczności lokalnej i problem ochrony danych osobowych

W związku z działaniami zapobiegającymi zakażeniu SARS CoV-2 instytucje publiczne, w tym w szczególności organy samorządowe, obarczone zostały dodatkowymi obowiązkami. Jednocześnie chęć niesienia pomocy społeczności lokalnej spowodowała powstanie wielu inicjatyw na rzecz wsparcia osób dotkniętych obostrzeniami z tytułu prewencji rozprzestrzeniania się zakażenia.

Uczestnicy Akademii Samorządowej sformułowali wiele wątpliwości, które dotyczą wszystkich jednostek samorządów lokalnych zaangażowanych w pomoc osobom dotkniętym epidemią (zarówno chorym, jak i zdrowym). Większość z tych uwag dotyczyła ujawniania i przepływu informacji między organami centralnymi a jednostkami samorządowymi. Pytania obejmowały w szczególności kwestie związane z brakiem informowania np. sołtysa o objęciu kwarantanną lub nadzorem epidemiologicznym konkretnych mieszkańców, z ujawnianiem listy wszystkich mieszkańców wraz z adresami i datami urodzenia czy też z ujawnianiem adresów seniorów w celu organizacji pomocy i wsparcia w związku z podejmowaniem środków prewencyjnych zakażeniu SARS CoV-2. Poniżej przedstawiamy wybrane pytania wraz z odpowiedziami.

Pytanie: *„Nikt też nas nie informuje, czy w sołectwie są jakieś osoby na kwarantannie lub objęte nadzorem epidemiologicznym. Odbieram telefony od mieszkańców z pytaniem, czy pani X*

11 Tamże.

skończyła się już kwarantanna, bo była w sklepie wiejskim, a ja nie mam nawet pojęcia, że była objęta kwarantanną".

Udostępnienie danych osobowych jest jedną z czynności przetwarzania danych. Zgodnie z zasadą legalności, przetwarzanie danych jest zgodne z prawem, gdy posiada umocowanie w przepisach powszechnie obowiązujących. W myśl art. 6 r.o.d.o. przetwarzanie danych osobowych jest więc zgodne z prawem, gdy:

- osoba, której dane dotyczą, wyraziła na to zgodę,
- jest to niezbędne do realizacji umowy lub podejmowania działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest niezbędne dla realizacji ustawowych obowiązków administratora danych,
- jest niezbędne dla realizacji interesów publicznych lub sprawowania władztwa publicznego w ramach kompetencji administratora danych,
- jest niezbędne dla realizacji żywotnych interesów osoby, której dane dotyczą,
- jest niezbędne dla realizacji prawnie uzasadnionych interesów administratora lub innego podmiotu.

Informacja o objęciu konkretnej osoby kwarantanną lub nadzorem epidemiologicznym jest informacją o stanie zdrowia, a więc zgodnie z definicją zawartą w art. 4 pkt 15 r.o.d.o. są to dane dotyczące zdrowia. Zgodnie z art. 9 ust. 1 r.o.d.o. dane takie należą do szczególnych kategorii danych osobowych i co do zasady ich przetwarzanie w jakikolwiek sposób jest zabronione. Przewidziano jednak wyjątki pozwalające na odejście od tej zasady. Taki wyjątek ma miejsce np. w sytuacji, gdy przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przez poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnieniem wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej, przy czym przetwarzanie to musi odbywać się na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego UE. Co do zasady więc ujawnianie danych o personaliach osób objętych kwarantanną lub nadzorem epidemiologicznym jest możliwe tylko na podstawie ustawowego upoważnienia do przetwarzania tych danych przez konkretną jednostkę lub podmiot. Na dzień sporządzenia niniejszej opinii lokalni włodarze i jednostki samorządowe, w tym sołtysi, nie zostali ustawowo upoważnieni do pozyskiwania i dalszego przetwarza danych osobowych w związku z epidemią koronawirusa SARS CoV-2, tak więc praktyka nieinformowania sołtysów pozostaje prawidłowa.

W razie otrzymywania takich informacji i pytań od mieszkańców, jak wskazane powyżej, prawidłowym postępowaniem jest przekierowanie osoby pytającej do lokalnej stacji epidemiologicznej lub służb porządkowych (np. policji).

Pytanie: *„Przed RODO dostawałam bez problemu listę mieszkańców z adresami i datami urodzenia. Teraz jest to niemożliwe. Bazuję na starych listach i doświadczeniu, bo to nie jest pierwsza moja kadencja. Nie wiem, jak teraz może skutecznie działać nowy sołtys w większej wiosce".*

Ani „przed RODO", czyli przed 25 maja 2018 roku, ani po tej dacie nie ma i nie było prawnych możliwości dopuszczających udostępnianie sołtysowi danych osobowych wszystkich mieszkańców. Jak wskazano powyżej, udostępnienie danych jest jedną z czynności ich przetwarzania, tak więc posiada swoją prawną podstawę legalizującą. W tym przypadku nie ma ani podstawy prawnej, ani zasadności udostępniania pełnej listy mieszkańców lokalnym jednostkom samorządowym, szczególnie w bliżej nieokreślonym celu.

Kolejną kwestią jest niedookreślony cel pozyskania takiej listy mieszkańców. Zgodnie z zasadą ograniczenia celu, wyrażoną w art. 5 ust. 1 lit. b) r.o.d.o., przetwarzanie danych jest zgodne z prawem, jeżeli dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach. Pozyskanie pełnej listy mieszkańców z adresami i datami urodzenia nie znajduje uzasadnienia w ustawowych obowiązkach tych jednostek, zatem dane te byłyby przetwarzane z naruszeniem zasady ograniczenia celu przetwarzania.

Pytanie: *„Urząd gminy nie poda adresów seniorów w ogóle, żeby np. sprawdzić, czy wszystko mają. Mówię tutaj ogólnie o liście adresów seniorów dla, np. sołtysów lub wolontariuszy".*

Ponownie – dla legalności pozyskania i dalszego przetwarzania takich danych niezbędna jest odpowiednia podstawa prawna. Urząd gminy powinien być legitymowany do udostępnienia takich informacji sołtysowi, sołtys zaś uprawniony do ich przetwarzania w konkretnych celach. Obecnie nie ma w systemie prawnym przepisów umożliwiających urzędowi gminy udostępnienie takich danych, a sołtysom ich dalsze przetwarzanie.

Pytanie: *„Paczki żywnościowe dla odbywających kwarantannę: urząd nie podawał przyczyn dostarczania paczki (w pierwszych tygodniach), zatem nie było pewności, czy jest to osoba zakażona, starsza, czy też taka, która wróciła z podróży. Było to w czasie, gdy te paczki podawało się do rąk. Ale to chyba nie podpada pod RODO".*

Wątpliwości wyrażone w tym pytaniu skupiają się na zagadnieniu, czy fizyczne dostarczanie paczki jest ujawnieniem danych. Takie działania nie powinny być jednak rozważane na gruncie r.o.d.o. – chodzi tu o realizację konkretnych działań, które mogłyby obserwować osoby postronne, na co nie ma wpływu podmiot odpowiedzialny za te działania. W czasie powszechnej kwarantanny zwiększa się typowa sąsiedzka ciekawość, więc niezależnie od przyjętych środków bezpieczeństwa, nie ma możliwości uniknięcia bycia zaobserwowanym. Nie stanowi to jednak ujawnienia danych osobowych.

Agnieszka Krzyżak – prawniczka w kancelarii Barta Litwiński Kancelaria Radców Prawnych i Adwokatów sp. p. Członkini SABI – Stowarzyszenia Inspektorów Ochrony Danych. Specjalizuje się w prawie ochrony danych osobowych, prawie autorskim oraz prawie ochrony konkurencji i konsumentów.

Paweł Litwiński – adwokat, partner w kancelarii Barta Litwiński Kancelaria Radców Prawnych i Adwokatów sp. p. Dyrektor Zarządzający w Instytucie Prawa Nowych Technologii i Ochrony Danych Osobowych Uczelni Łazarskiego. Członek Grupy Ekspertów Komisji Europejskiej do spraw wdrożenia ogólnego rozporządzenia o ochronie danych osobowych (RODO).

Przykładowe procedury, jakie można wprowadzić w zakresie zabezpieczenia obiegu korespondencji i danych w urzędzie

Aneks 1

Procedura wewnętrzna:

zasady wynoszenia dokumentów papierowych oraz wykorzystywania elektronicznych nośników informacji przy transmisji informacji poza obszar przetwarzania danych.

ZWERYFIKOWAŁ		ZATWIERDZIŁ	
DATA	PODPIS	DATA	PODPIS

Wstęp

Cel procedury[1]

1. W związku z dynamicznie rozwijającą się i pogarszającą sytuacją, związaną z rozprzestrzenianiem się zakażenia wirusem SARS CoV-2, mając na względzie bezpieczeństwo oraz zdrowie i życie ludzi, uwzględniając rekomendacje Światowej Organizacji Zdrowia (World Health Organization, WHO) i Centers for Disease Control and Prevention (CDC), [*nazwa jednostki, np. Miejski Dom Kultury*] zdecydował o oddelegowaniu pracowników i osób świadczących usługi na jego rzecz do realizacji obowiązków w formie pracy zdalnej.

2. Realizacja obowiązków służbowych z uwagi na wyżej wskazane okoliczności wymaga wynoszenia poza obszar przetwarzania danych osobowych określonych w wewnętrznych politykach [*nazwa jednostki, np. Miejski Dom Kultury*] nośników zawierających dane osobowe.

3. Niniejsza Procedura wewnętrzna (dalej jako **Procedura**) określa zasady wynoszenia dokumentów papierowych oraz wykorzystywania elektronicznych nośników informacji przy transmisji informacji poza obszar przetwarzania danych w [*nazwa jednostki, np. Miejski Dom Kultury, adres i dane identyfikujące jednostkę*] (dalej jako **Jednostka**), ze szczególnym uwzględnieniem konieczności zapewnienia poufności informacji, w tym danych osobowych, utrwalonych lub zapisanych na tych nośnikach.

Przedmiot procedury i podmioty odpowiedzialne

1. Zasady postępowania ustalone w niniejszej Procedurze mają zastosowanie do wszystkich dokumentów zawierających dane osobowe oraz inne informacje, które ze względu na swoją treść muszą pozostać poufne[2] (w tym informacje sklasyfikowane co najmniej jako zastrzeżone zgodnie z klasyfikacją informacji wynikającą z ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych).

1 Procedura została opracowana jako uregulowanie szczególnych rozwiązań w związku z prewencją rozprzestrzeniania się zakażenia. Postanowienia procedury można jednak przyjąć jako standardy postępowania w organizacji również po ustaniu stanu epidemii.

2 Postanowienie do decyzji podmiotu: rozszerzyć zastosowanie czy pozostać wyłącznie przy danych osobowych.

2. Zasady postępowania ustalone w niniejszej Procedurze mają zastosowanie do wszystkich elektronicznych nośników informacji, na których utrwalone lub zapisane zostały dane osobowe oraz inne informacje, które ze względu na swoją treść muszą pozostać poufne[3] (w tym informacje sklasyfikowane co najmniej jako zastrzeżone zgodnie z klasyfikacją informacji wynikającą z ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych), w tym w szczególności pendrive'y.

3. Niniejsza Procedura określa prawa i obowiązki podmiotów świadczących na rzecz Jednostki, w tym pracowników i współpracowników Jednostki, niezależnie od stopnia zaangażowania tych osób, zakresu obowiązków pełnionych na rzecz Jednostki oraz stosunku prawnego wiążącego te osoby z Jednostką (stosunek pracy, umowy cywilnoprawne, wolontariat, praktyka) – dalej zwanych pracownikami.

Zasady postępowania z dokumentami papierowymi wynoszonymi poza obszar przetwarzania danych osobowych

Transport dokumentacji

1. Jeżeli dla realizacji obowiązków służbowych pracownik musi wynieść dokumenty poza obszar przetwarzania danych osobowych, pracownik zgłasza ten fakt bezpośredniemu przełożonemu (obowiązek informacyjny). Zgłoszenie takie może być dokonane również w formie elektronicznej lub w rozmowie telefonicznej/wiadomości SMS.

2. Pracownik wynoszący dokumenty zobowiązany jest przed opuszczeniem obszaru przetwarzania danych do zabezpieczenia treści dokumentów, np. poprzez zamknięcie ich w teczce lub kopercie tak, aby uniemożliwić osobom postronnym odczytanie treści dokumentów podczas ich transportu. Pracownik nie powinien transportować dokumentów w przezroczystych opakowaniach czy koszulkach.

3. Pracownik wynoszący dokumenty jest odpowiedzialny za zapewnienie ich poufności i integralności, w tym za zachowanie szczególnej ostrożności podczas ich transportu.

4. Zabrania się otwierania lub przeglądania dokumentów w miejscach publicznych, w tym rozrywania kopert, jeżeli dokumenty transportowane są w kopertach.

5. Zabrania się zapoznawania z treścią dokumentów w miejscach publicznych, w tym odczytywania ich w autobusach lub na przystankach, gdzie osoby postronne mogą również zaznajomić się z treścią dokumentów.

6. Zabrania się pozostawiania dokumentów bez nadzoru, np. na siedzeniu samochodu czy w autobusie.

Po dotarciu do miejsca, gdzie wykonywana ma być praca zdalna, lub celu, do którego dokumenty były transportowane, pracownik weryfikuje, czy transportowany zbiór jest kompletny i nie został uszkodzony (np. zalany). W przypadku stwierdzenia nieprawidłowości, w szczególności braków w dokumentacji, pracownik bezzwłocznie informuje bezpośredniego przełożonego o braku oraz zobowiązany jest zastosować się do wewnętrznych procedur postępowania przewidzianych dla sytuacji naruszenia

3 Postanowienie do decyzji podmiotu: rozszerzyć zastosowanie czy pozostać wyłącznie przy danych osobowych.

bezpieczeństwa informacji, a jeżeli dokumenty zawierały dane osobowe – naruszenia ochrony danych osobowych.

Postępowanie z dokumentacją poza obszarem przetwarzania danych osobowych

1. Dokumenty wyniesione poza obszar przetwarzania danych osobowych należy zabezpieczyć przed zniszczeniem, uszkodzeniem, zdekompletowaniem, możliwością zapoznania się z ich treścią przez osoby postronne, w tym przez domowników i współlokatorów pracownika.

2. W przypadku czasowego zawieszenia pracy dokumenty należy zabezpieczyć. Zabrania się pozostawiania wyniesionej dokumentacji na widoku, w zasięgu osób postronnych, w tym domowników i współlokatorów pracownika.

3. Po zakończonej pracy dokumenty należy zabezpieczyć. Zabrania się pozostawiania wyniesionej dokumentacji na widoku, w zasięgu osób postronnych, w tym domowników i współlokatorów pracownika.

4. W przypadku stwierdzenia nieprawidłowości, w szczególności braków w dokumentacji lub jej uszkodzenia albo zdekompletowania, pracownik musi bezzwłocznie poinformować bezpośredniego przełożonego o braku oraz zobowiązany jest zastosować się do wewnętrznych procedur postępowania przewidzianych dla sytuacji naruszenia bezpieczeństwa informacji, a jeżeli dokumenty zawierały dane osobowe – naruszenia ochrony danych osobowych.

Zasady postępowania z nośnikami elektronicznymi i optycznymi, służącymi do transportu informacji, w tym danych osobowych, poza obszar przetwarzania danych

Nośniki zewnętrzne dopuszczone do użytku w Jednostce, ich konfiguracja i dopuszczalność wykorzystania

1. Jeżeli zostaną uwzględnione postanowienia niniejszego działu Procedury, dopuszcza się używanie służbowych oraz prywatnych urządzeń umożliwiających przenoszenie i archiwizowanie danych, w tym nagrywarek CD/DVD, nośników zewnętrznych typu płyt CD i DVD, dysków zewnętrznych oraz nośników typu pendrive, należy jednak unikać przechowywania ważnych danych na tego typu nośnikach zewnętrznych bez wyraźnej potrzeby. W szczególności należy unikać przechowywania na takich nośnikach danych osobowych, o ile nie jest to bezwzględnie konieczne.

2. Do wykorzystania nośników, o których mowa wyżej, potrzebna jest zgoda kierownika Jednostki.

3. Pracownik, który musi wykorzystywać zewnętrzne nośniki do przechowywania danych, w szczególności danych osobowych, zobowiązany jest zgłosić ten fakt kierownikowi Jednostki i uzyskać jego zgodę na wykorzystywanie wskazanego nośnika. Zgoda musi być wyrażona przynajmniej w formie elektronicznej (wiadomości e-mail), tak aby możliwe było jej udokumentowanie na potrzeby realizacji zasady rozliczalności.

4. W przypadku konieczności przechowywania na nośnikach, o których mowa powyżej w ust. 1, ważnych danych, w szczególności w przypadku przechowywania na takich nośnikach danych osobowych, konieczne jest stosowanie wobec tych nośników środków ochrony kryptograficznej (szyfrowania). Zgoda kierownika Jednostki na użytkowanie nośnika jest zawsze wydawana pod warunkiem zaszyfrowania nośnika.

5. Pracownik, który będzie korzystał z nośnika, o którym mowa w ust. 1., zobowiązany jest dostarczyć nośnik przed rozpoczęciem używania do administratora systemów informatycznych (ASI), a jeżeli w Jednostce nie została wyznaczona taka osoba, do dyżurującego informatyka Jednostki. Za odpowiednie zaszyfrowanie nośnika odpowiedzialny jest ASI, a jeżeli w Jednostce nie została wyznaczona taka osoba, dyżurujący informatyk Jednostki.

6. Nośniki zewnętrzne, na których znajdują się ważne dane (w szczególności dane osobowe) zaszyfrowane przez ASI lub dyżurnego informatyka Jednostki, są oznaczane w sposób trwały, jednoznaczny i czytelny. Tak oznaczone nośniki są ewidencjonowane w rejestrze nośników komputerowych zawierających ważne dane[4].

7. Za prowadzenie rejestru nośników komputerowych odpowiedzialny jest ASI lub oddelegowany informatyk Jednostki.

Dopuszczalne wykorzystanie nośników zewnętrznych i transport

1. Na czas stosowania szczególnych środków związanych z rozprzestrzenianiem się zakażenia SARS CoV-2 uchyla się zakaz wykorzystywania nośników zewnętrznych do przenoszenia danych na prywatne komputery lub inne urządzenia mogące służyć do przechowywania danych, pozostające poza kontrolą Jednostki pod następującymi warunkami:
   1.1. Pracownik został oddelegowany do pracy zdalnej lub w porozumieniu z Jednostką podejmuje pracę w formie zdalnej.
   1.2. Pracownik w porozumieniu z Jednostką wykorzystuje prywatny sprzęt komputerowy lub inne urządzenie prywatne w celu realizacji obowiązków służbowych na rzecz Jednostki.
   1.3. Prywatny sprzęt komputerowy lub inne urządzenie prywatne spełnia minimalne wymogi bezpieczeństwa wskazane przez Jednostkę, tj. posiada aktualne oprogramowanie, w tym aktualny system operacyjny, posiada aktualne oprogramowanie antywirusowe skonfigurowane w taki sposób, aby aktualizacja oprogramowania oraz bazy sygnatur wirusów następowała automatycznie[5].

2. Zabrania się wykorzystywania nośników prywatnych przeznaczonych do transportu i zapisu danych i informacji w związku z realizacją obowiązków służbowych do celów prywatnych, w tym zapisywania na nich prywatnych informacji i treści, w szczególności pobieranych z Internetu.

3. Za nadzór nad przekazanymi pracownikowi nośnikami, w szczególności za zapewnienie bezpieczeństwa nośników i poufności zawartych na nich informacji, odpowiedzialność ponosi pracownik dysponujący nośnikiem.

4 Należy opracować system rejestrowania i ewidencjonowania nośników, które są wykorzystywane w Jednostce.
5 Postanowienie do decyzji podmiotu: można rozszerzyć o dodatkowe wymogi, które będą budowały bezpieczeństwo danych.

4. Po zakończeniu pracy przez pracownika wymienne nośniki zewnętrzne są przechowywane w miejscach zapewniających ich bezpieczeństwo i poufność zapisanych na nich informacji, w tym danych osobowych.

5. Nośniki zewnętrzne transportuje się w sposób bezpieczny, tj. tak, by pozostawały pod stałym nadzorem, nie były pozostawiane w miejscach widocznych, np. w samochodach, przypięte do pasków, kluczy itp.

Postanowienia końcowe

1. Terminy i pojęcia użyte w niniejszej Procedurze, o ile z jej treści nie wynika inaczej, mają znaczenie takie, jakie wynika z przepisów prawa powszechnie obowiązującego.

2. W zakresie nieuregulowanym w niniejszej Procedurze zastosowanie mają przepisy prawa powszechnie obowiązującego, w szczególności dotyczące postępowania z informacjami o charakterze niejawnym oraz danymi osobowymi, w tym rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) oraz ustawy z dnia 14 czerwca 1960 roku – Kodeks postępowania administracyjnego.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Procedury mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która będąc zobowiązana do podjęcia określonych działań, nie wypełnia tych obowiązków lub uchyla się od ich wypełnienia[6].

4. Wobec osoby, która zobowiązana nie podjęła działania określonego w Procedurze, wszczyna się postępowanie oraz nakłada na nią karę wynikającą w ogólnych zasad odpowiedzialności. Powyższe nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującymi przepisami prawa oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego o rekompensatę z tytułu poniesionych strat lub wyrządzonej krzywdy.

5. Wdrożenie Procedury oraz działania korygujące i zachowawcze odbywają się poprzez zapoznanie z treścią Procedury pracowników i współpracowników Jednostki (świadczących zadania na innej podstawie niż umowa o pracę).

6. Procedura wchodzi w życie z dniem zatwierdzenia przez kierownika Jednostki i obowiązuje do czasu jej uchylenia w związku z ustąpieniem stanu epidemii[7]. Uchylenie Procedury następuje w formie zarządzenia kierownika Jednostki.

6 Pkt 3 i 4 sankcjonowanie naruszeń – w trybie możliwości, nie nakazu, tak więc do decyzji kierownika, czy takie konsekwencje naruszania procedury będą stosowane, nawet przy pozostawieniu tych postanowień.

7 Uwaga: procedura na okres pandemii. Należy pamiętać o jej uchyleniu.

Aneks 2

Procedura wewnętrzna:

szczególne środki bezpieczeństwa w służbie prewencji zakażeniom SARS CoV-2 w związku z obiegiem korespondencji przychodzącej.

ZWERYFIKOWAŁ		ZATWIERDZIŁ	
DATA	PODPIS	DATA	PODPIS

Wstęp

Cel procedury

1. W związku z dynamicznie rozwijającą się i pogarszającą sytuacją, związaną z rozprzestrzenianiem się zakażenia wirusem SARS CoV-2, mając na względzie bezpieczeństwo oraz zdrowie i życie ludzi i uwzględniając rekomendacje Światowej Organizacji Zdrowia (World Health Organization, WHO) oraz Centers for Disease Control and Prevention (CDC), [*nazwa jednostki, np. Miejski Dom Kultury*] zdecydował o wprowadzeniu zasad postępowania, mających na celu minimalizację zagrożeń związanych z zakażeniem.

2. Niniejsza Procedura wewnętrzna w sprawie szczególnych środków bezpieczeństwa w służbie prewencji zakażeniom wirusem SARS CoV-2 w związku z obiegiem korespondencji przychodzącej (dalej jako **Procedura**) ma na celu usystematyzowanie i ujednolicenie zasad dotyczących podejmowania i dalszej dystrybucji korespondencji przychodzącej w [*nazwa jednostki, np. Miejski Dom Kultury, adres i dane identyfikujące jednostkę*] (dalej jako **Jednostka**).

Przedmiot procedury i podmioty odpowiedzialne

1. Zasady postępowania ustalone w niniejszej Procedurze mają zastosowanie do wszelkiej korespondencji przychodzącej i dostarczanej do Jednostki, zarówno do siedziby głównej, jak również do filii czy oddziałów terenowych.

2. Zasady postępowania ustalone w niniejszej Procedurze mają zastosowanie do korespondencji przychodzącej niezależnie od podmiotu odpowiedzialnego za jej dostarczenie do Jednostki, w tym do jej siedziby głównej, jak również filii czy oddziałów terenowych. Bez znaczenia dla stosowania niniejszych zasad pozostaje również, czy podmiot dostarczający korespondencję jest operatorem rejestrowym, wyznaczonym, czy działa na podstawie innych przepisów prawa powszechnie obowiązującego.

3. Dla uniknięcia wątpliwości, za korespondencję przychodzącą uznaje się zarówno korespondencję w formie listów tradycyjnych, jak również paczek i przesyłek, w tym dostarczanych transportem kurierskim, wyłączając korespondencję przekazywaną bezpośrednio między pracownikami Jednostki, w tym dokumentów transportowanych przez pracowników Jednostki z jednego oddziału lub filii do drugiego.

4. Niniejsza Procedura określa prawa i obowiązki podmiotów zaangażowanych w przyjmowanie i dalszą dystrybucję korespondencji przychodzącej adresowanej do Jednostki, jak również innych pracowników i współpracowników Jednostki, niezależnie od stopnia zaangażowania tych osób w proces obiegu korespondencji w Jednostce, zakresu obowiązków pełnionych poza procesem obiegu korespondencji oraz stosunku prawnego wiążącego te osoby z Jednostką (stosunek pracy, umowy cywilnoprawne, wolontariat, praktyka) – dalej zwanych **Pracownikami**.

Zasady podejmowania korespondencji przychodzącej

1. Przyjmowaniem korespondencji przychodzącej zajmuje się [*należy wskazać kategorie osób odpowiedzialnych za podejmowanie korespondencji w Jednostce*].

2. Pracownik przyjmujący korespondencję zobowiązany jest opatrzyć ją datą wpływu do Jednostki, a jeśli w Jednostce prowadzona jest książka korespondencyjna, również wpisać odpowiednią pozycję do tej książki[1].

Podejmowanie korespondencji zwykłej i niewymagającej pokwitowania

1. Przyjmowanie **listów zwykłych** oraz przesyłek niewymagających pokwitowania odbywa się poprzez wyjęcie ich z fizycznej skrzynki odbiorczej (podawczej).

2. W przypadku gdy osoba przynosząca wiadomość zgłasza się bezpośrednio do Jednostki, winna ona umieścić korespondencję w przeznaczonej do tego skrzynce odbiorczej (podawczej). Adekwatna informacja o osobistym doręczaniu przesyłek niewymagających potwierdzenia czy pokwitowania, w tym zawierająca opis miejsca, gdzie znajduje się skrzynka odbiorcza (podawcza), powinna zostać podana do wiadomości publicznej w taki sposób, aby umożliwić zapoznanie się z nią wszystkim zainteresowanym[2].

3. Podejmując korespondencję zwykłą (wyciągając korespondencję ze skrzynki podawczej), Pracownik zobowiązany jest używać rękawiczek ochronnych.

Podejmowanie korespondencji poleconej i wymagającej pokwitowania

1. Korespondencję poleconą oraz wymagającą pokwitowania przyjmuje się poprzez bezpośrednie fizyczne przejęcie listu lub przesyłki od osoby przynoszącej wiadomość bezpośrednio do Jednostki.

2. W przypadku podejmowania **listów poleconych** oraz przesyłek wymagających pokwitowania, wprowadza się następujące zasady podejmowania korespondencji:
   2.1. Podejmując korespondencję, Pracownik zobowiązany jest używać rękawiczek ochronnych.
   2.2. W przypadku gdy korespondencja dostarczana jest osobiście z rąk do rąk, Pracownik jest dodatkowo zobowiązany do użycia maseczki ochronnej.
   2.3. Przyjmując korespondencję, Pracownik jest zobowiązany do utrzymania maksymalnego odstępu od osoby ją dostarczającej. Odstęp ten powinien wynosić minimum 2 metry. Jeżeli niemożliwe jest zachowanie bezpiecznego odstępu, należy poinstruować przynoszącego wiadomość,

1 Postanowienie do decyzji podmiotu. Jego wprowadzenie ogranicza listę osób odpowiedzialnych za rejestrowanie obiegu korespondencji.
2 Postanowienie do decyzji podmiotu, który tworzy procedurę.

aby położył korespondencję na stole, ladzie lub innej powierzchni. Powierzchnię tę należy uprzednio zabezpieczyć np. folią. Korespondencję można podjąć dopiero po tym, jak przynoszący odsunie się na bezpieczną odległość, wynoszącą minimum 2 metry.

2.4. W przypadku konieczności pokwitowania odbioru, należy wszelkie druki podpisywać w miarę możliwości własnym długopisem, pamiętając o zachowaniu bezpiecznej odległości od dostarczyciela.

3. Korespondencję należy przyjmować sprawnie, maksymalnie ograniczając czas przebywania osób postronnych w pomieszczeniu.

Postępowanie po podjęciu korespondencji przychodzącej

1. Bezpośrednio po podjęciu korespondencji przychodzącej, korespondencja powinna być złożona w miejscu wyznaczonym przez kierownika Jednostki lub przygotowana do dalszej dystrybucji, o ile zastosowania nie mają szczególne regulacje dotyczące pozostawienia korespondencji w kwarantannie po momencie jej podjęcia.

2. Pracownik podejmujący po zakończeniu swoich czynności powinien zdjąć w sposób bezpieczny rękawiczki ochronne, a następnie umyć i zdezynfekować dłonie i przedramiona zgodnie z instrukcją bezpiecznego mycia i dezynfekcji rąk.

3. Pracownik podejmujący korespondencję przychodzącą poleconą lub wymagającą pokwitowania zdejmuje maseczkę ochronną dopiero po dokładnej dezynfekcji rąk.

4. Zużyte rękawiczki i maseczka ochronna powinny od razu zostać wyrzucone do specjalnie do tego przeznaczonego pojemnika, zawierającego materiał potencjalnie niebezpieczny, przeznaczony do utylizacji. Zabrania się wyrzucania zużytych materiałów ochronnych bezpośrednio do koszy na śmieci znajdujących się przy biurkach[3].

5. Nie należy dłoni i przedramion zbliżać do twarzy lub otwartych ran, zadrapań, skaleczeń. Stanowczo zabrania się zdejmowania maseczki ochronnej przed dokładnym umyciem i dezynfekcją rąk.

6. Instrukcja poprawnego mycia i dezynfekcji rąk znajduje się w załączeniu do niniejszej Procedury oraz podawana jest do wiadomości wszystkich pracowników poprzez wywieszenie jej w strategicznych miejscach Jednostki, w szczególności w łazienkach[4].

Zasady dalszej dystrybucji korespondencji przychodzącej

1. Jakiekolwiek działania podejmowane z podjętą korespondencją powinny mieć miejsce wyłącznie z wykorzystaniem rękawiczek ochronnych.

2. Kierownik Jednostki może wprowadzić szczególne regulacje dotyczące pozostawienia korespondencji w kwarantannie. W takim przypadku przez okres pomiędzy podjęciem korespondencji a przygotowaniem jej do dalszej dystrybucji korespondencja nie powinna być dotykana, przesuwana czy otwierana[5].

3 Postanowienie do decyzji podmiotu, który tworzy procedurę.
4 W załączniku przykład ulotki przygotowanej przez Główny Inspektorat Sanitarny.
5 Kwarantanna będzie skuteczna, jeżeli jej okres wyniesie nie mniej niż 17 dni.

3. W sytuacji przypadkowego lub intencjonalnego kontaktu pracownika z podjętą korespondencją pozostającą w kwarantannie adekwatne zastosowanie mają zasady postępowania wskazane dla działań podejmowanych po podjęciu korespondencji przychodzącej.

Otwieranie korespondencji i przygotowywanie do dalszej dystrybucji wewnętrznej[6]

1. Wyznaczony pracownik Jednostki, wykorzystując rękawiczki ochronne, otwiera koperty zawierające korespondencję przychodzącą w formie listów zwykłych oraz paczki i przesyłki otrzymane przez Jednostkę.

2. Wyznaczenie pracownika lub pracowników w Jednostce, którzy będą uprawnieni i odpowiedzialni za otwieranie i przygotowanie korespondencji do dalszej dystrybucji, odbywa się za pomocą wzoru upoważnienia, który stanowi załącznik nr 2 do niniejszej Procedury.

3. Zachowując szczególną ostrożność, pracownik wykonuje skany korespondencji przychodzącej.

4. Pracownik przygotowujący korespondencję do dalszej dystrybucji po wykonaniu skanu chowa korespondencję do koperty lub opakowania, w którym została ona podjęta, i składa ją w miejscu wyznaczonym przez kierownika Jednostki[7].

Dalsza dystrybucja wewnętrzna korespondencji przychodzącej

1. Zapisane skany pracownik przesyła do wydziału lub oddziału/filii Jednostki, która jest bezpośrednim adresatem korespondencji lub która jest odpowiedzialna za dalsze kroki podejmowane w związki z treścią korespondencji.

2. Wysyłka odbywa się pocztą elektroniczną na odpowiednie adresy e-mail wewnętrznej poczty elektronicznej.

3. Pracownik dokonujący dalszej dystrybucji korespondencji jest zobowiązany do weryfikacji, czy adres e-mail jest poprawny i czy znajduje się w wewnętrznej domenie Jednostki. W przypadku zidentyfikowania nieprawidłowości lub braku możliwości dokonania dalszej dystrybucji korespondencji pracownik zgłasza problem kierownikowi Jednostki. Kierownik Jednostki podejmuje decyzję co do sposobu dalszej dystrybucji korespondencji.

4. Po realizacji swoich obowiązków, pracownik zobowiązany jest do podjęcia kroków wskazanych dla działań podejmowanych po podjęciu korespondencji przychodzącej.

5. Korespondencja w formie fizycznej nie jest dystrybuowana wewnętrznie, o ile kierownik Jednostki nie podejmie stosownej decyzji o konieczności dostarczenia korespondencji w formie fizycznej bezpośrednio do danego wydziału.

6. W przypadku bezpośredniej fizycznej dystrybucji do danego wydziału, adekwatne zastosowanie mają zasady postępowania wskazane dla działań podejmowanych po podjęciu korespondencji przychodzącej.

6 Dotyczy skanowania dokumentów papierowych – do decyzji kierownika jednostki, czy będzie miało ono miejsce.
7 Postanowienie do decyzji podmiotu, który tworzy procedurę.

Postanowienia końcowe

1. Terminy i pojęcia użyte w niniejszej Procedurze, o ile z treści Procedury nie wynika inaczej, mają znaczenie takie, jakie wynika z przepisów prawa powszechnie obowiązującego.

2. W zakresie nieuregulowanym w niniejszej Procedurze zastosowanie mają przepisy prawa powszechnie obowiązującego, w szczególności dotyczące postępowania z informacjami o charakterze niejawnym oraz danymi osobowymi, w tym rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) oraz ustawy z dnia 14 czerwca 1960 roku – Kodeks postępowania administracyjnego.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Procedury mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która jako zobowiązana do podjęcia określonych działań nie wypełnia tych obowiązków lub uchyla się od ich wypełnienia.

4. Wobec osoby, która zobowiązana nie podjęła działania określonego w Procedurze, wszczyna się postępowanie oraz nakłada na nią karę wynikającą w ogólnych zasad odpowiedzialności. Powyższe nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującymi przepisami prawa oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego o rekompensatę z tytułu poniesionych strat lub wyrządzonej krzywdy[8].

5. Wdrożenie Procedury oraz działania korygujące i zachowawcze odbywają się poprzez zapoznanie z treścią Procedury pracowników i współpracowników Jednostki (świadczących zadania na innej podstawie niż umowa o pracę).

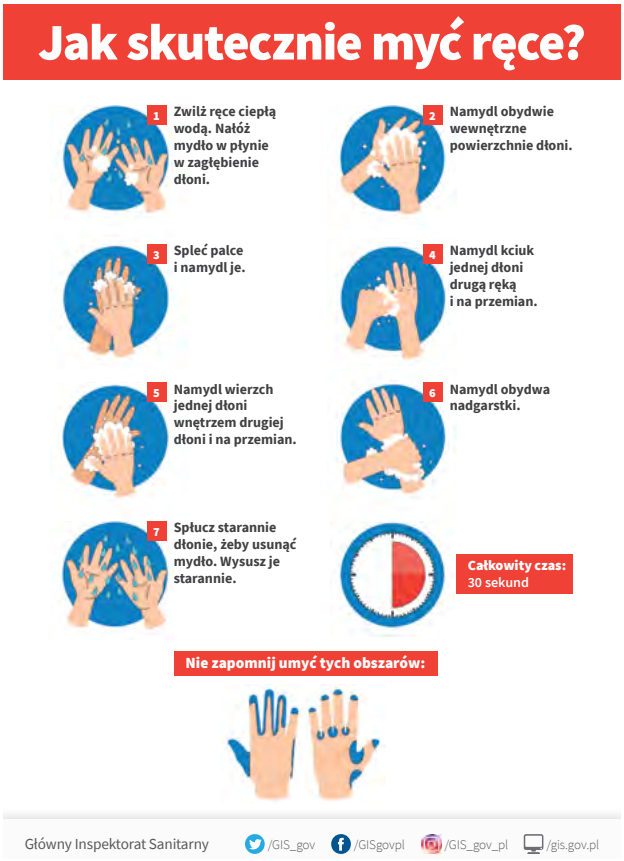
6. Procedura wchodzi w życie z dniem zatwierdzenia przez kierownika Jednostki i obowiązuje do czasu jej uchylenia w związku z ustąpieniem stanu epidemii. Uchylenie Procedury następuje w formie Zarządzenia kierownika Jednostki.

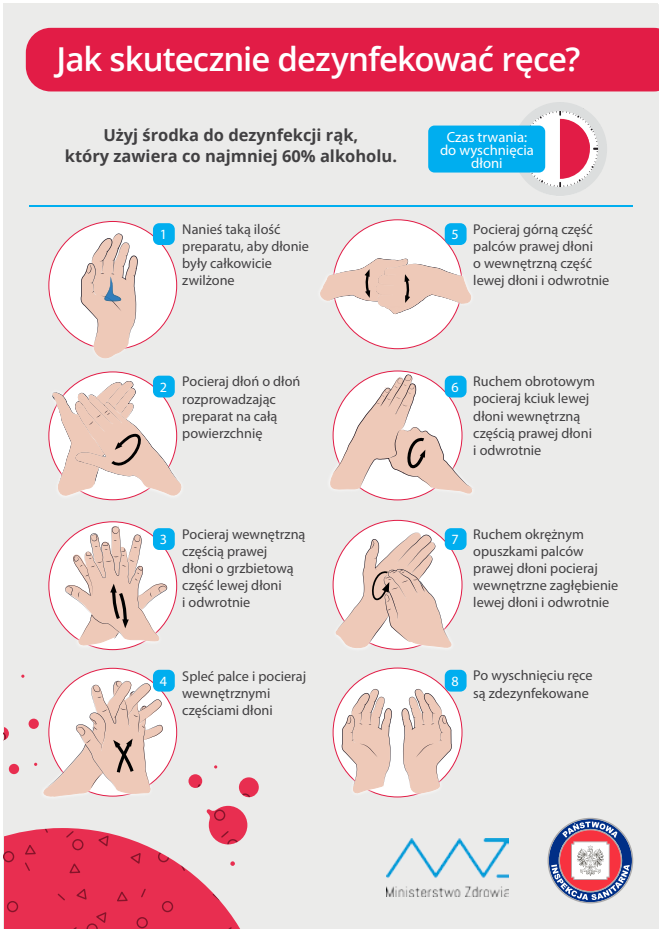
Załącznik nr 1 – Infografiki dotyczące bezpiecznego mycia i dezynfekcji rąk (GIS).

Załącznik nr 2 – Wzór upoważnienia do otwierania i dalszej dystrybucji korespondencji.

8 Do decyzji kierownika, czy takie konsekwencje niestosowania procedury będą stosowane, nawet przy pozostawieniu tych postanowień.

Załącznik nr 1 – Infografiki dotyczące bezpiecznego mycia i dezynfekcji rąk.





Załącznik nr 2 – Wzór upoważnienia do otwierania i dalszej dystrybucji korespondencji.

[*miejscowość*], [*data*]

Upoważnienie do przetwarzania danych osobowych

nr [_____]

Działając w imieniu Administratora Danych Osobowych, [*nazwa Jednostki*], niniejszym upoważniam

[*imię i nazwisko*], [*stanowisko*]

do przetwarzania danych osobowych w [*nazwa Jednostki*], w zakresie niezbędnym do realizacji szczególnych środków bezpieczeństwa w służbie prewencji zakażeniom wirusem SARS CoV-2 w związku z obiegiem korespondencji przychodzącej w [*nazwa Jednostki*].

Upoważnienie dotyczy przetwarzania danych osobowych w imieniu i na zlecenie Administratora Danych Osobowych, w związku z realizacją szczególnych obowiązków jako osoby odpowiedzialnej za przygotowanie korespondencji przychodzącej do dalszej dystrybucji, w tym jej segregację, skanowanie oraz przesyłanie odpowiednim adresatom korespondencji.

Upoważnienie jest ważne do momentu uchylenia Procedury wewnętrznej w sprawie szczególnych środków bezpieczeństwa w służbie prewencji zakażeniom wirusem SARS CoV-2 w związku z obiegiem korespondencji przychodzącej lub do momentu jego cofnięcia przez Administratora Danych Osobowych, i dotyczy danych udostępnianych Upoważnionemu w związku z realizacją operacji na danych, w ramach umocowania ADO.

ADO równocześnie zobowiązuje Upoważnionego do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzania danych osobowych oraz sposobu ich zabezpieczenia, a także postępowania z danymi, zgodnie z obowiązującymi u ADO unormowaniami, w szczególności zachowania ich poufności, integralności oraz właściwego ich zabezpieczenia. Powyższe podlega kontroli ADO.

Naruszenie obowiązków w zakresie ochrony danych osobowych, w szczególności ich udostępnienie lub umożliwienie dostępu do danych osobie nieupoważnionej, może skutkować nałożeniem na Upoważnionego kary porządkowej, a nawet rozwiązaniem stosunku wiążącego go z ADO bez wypowiedzenia z powodu ciężkiego naruszenia obowiązków. Podlega również odpowiedzialności cywilnej i karnej, zgodnie z przepisami prawa powszechnego.

.....

Upoważniający

_____

Oświadczenia Upoważnionego

Oświadczam, że zapoznałem się z zasadami ochrony danych osobowych w [*nazwa Jednostki*] oraz wdrożoną dokumentacją i procedurami dającymi gwarancje ochrony tych danych i zobowiązuję się do przestrzegania obowiązujących zasad przetwarzania danych osobowych, dołożenia wszelkiej staranności, by zapewnić ich ochronę i integralność, w szczególności zabezpieczyć je przed udostępnianiem osobom trzecim i nieuprawnionym lub przed nieautoryzowanym dostępem, zabraniem, uszkodzeniem, modyfikacją czy zniszczeniem.

Zobowiązuję się również do zachowania poufności przetwarzanych w imieniu ADO danych osobowych oraz nieujawniania osobom trzecim treści i informacji dotyczących danych czy innych informacji, których ujawnienie może w jakikolwiek sposób negatywnie wpłynąć na bezpieczeństwo przetwarzania danych bądź zasugerować ich treść, tak w trakcie trwania stosunku prawnego łączącego mnie z [*nazwa Jednostki*], jak i bezterminowo po ustaniu tego stosunku, jak również do niewykorzystywania tych informacji w sposób sprzeczny z treścią otrzymanego upoważnienia. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia integralności danych osobowych czy któregokolwiek elementu zabezpieczenia tych danych lub systemu informatycznego, zgodnie z procedurami obowiązującymi u ADO.

Oświadczam, że jestem świadomy obowiązku zachowania poufności, również po odwołaniu upoważnienia oraz po ustaniu stosunku prawnego łączącego mnie z ADO. Przyjmuję także do wiadomości, że naruszenie powyższych obowiązków może stanowić podstawę odpowiedzialności cywilnej i karnej oraz może zostać uznane za naruszenie treści stosunku prawnego łączącego mnie z ADO i w ten sposób może stanowić podstawę do natychmiastowego rozwiązania tego stosunku.

.....

Upoważniony

Fundacja im. Stefana Batorego
Sapieżyńska 10a
00-215 Warszawa
tel. (48-22) 536 02 00
fax (48-22) 536 02 20
batory@batory.org.pl
www.batory.org.pl

Koncepcja i redakcja merytoryczna: Anna Wawrzyniak
Redakcja językowa: Izabella Sariusz-Skąpska
Warszawa 2020
ISBN 978-83-66543-18-8