JUSTYNA JABŁONKA

Kwiecień 2023
Nr 2/2023

KANCELARIA WYRZYKOWSCY

Newsletter

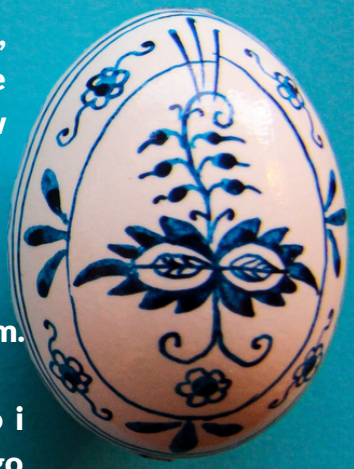
INSPEKTORA OCHRONY DANYCH

ADW. JUSTYNY JABŁONKI

Drodzy Administratorzy Danych,

w kolejnym, kwietniowym wydaniu Newsletter-a Inspektora Ochrony Danych, chcę przede wszystkim zwrócić Państwa uwagę na ważne aspekty w zakresie bezpieczeństwa przetwarzanych danych podczas korzystania z nośników zewnętrznych. Pozostałe kwestie, o których będzie mowa, ujęłam poniżej.

Pozostaje mi również przesłać Państwu życzenia na ten zbliżający się, wyjątkowy czas Wielkanocy:



... niech ten świąteczny czas napełni Państwa serca radością, nadzieją i pokojem. Niech w domu zagości uśmiech, dobre słowa i wspólne chwile z bliskimi. Niech radość zmartwychwstania Chrystusa przyniesie nadzieję na lepsze jutro i siłę do pokonywania trudności. Wszystkiego najlepszego w te święta i radosnego Alleluja!

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

W kwietniu rozmawiamy o:

I. Pendrive'y, USB-sticky, czy praca przy ich użyciu może być „niebezpieczna"? Kara pieniężna dla jednostki sektora finansów publicznych w wysokości 30.000 tyś. zł.- Decyzja PUODO z dnia 19 stycznia 2023 r., DKN.5131.12.2020

Zdaję sobie sprawę, że praca na dyskach zewnętrznych może być wygodnym sposobem przenoszenia danych między różnymi urządzeniami, ale zwracam tym samym uwagę, iż wiąże się to również z pewnymi ryzykami związanymi z bezpieczeństwem danych.

Temat na tyle istotny, a tym samym zalecenie PUODO w wydanej decyzji godne uwagi, że postanowiłam poświęcić temu zagadnieniu więcej miejsca.

I.Naruszenie – w punktach:

1.Kto zgłosił naruszenie?
Sam Administrator: Sąd Rejonowy Szczecin-Centrum w Szczecinie, dalej jako: Sąd.

2. Na czym polegało naruszenie?
Zaginięcie z pomieszczania, w którym pracownik – X, wykonywał pracę, saszetki zawierającej trzy nośniki danych, jeden szyfrowany (służbowy) i dwa nieszyfrowane (prywatne).

3. Jakie dane osobowe znajdowały się na zagubionych nośnikach?
Dane zawarte w projektach orzeczeń i uzasadnień sporządzanych przez X w okresie od grudnia 2004 r. do sierpnia 2020 r., tj.: imiona i nazwiska, adresy zamieszkania lub pobytu, dane dotyczące zakładu pracy oraz dane dotyczące zdrowia.

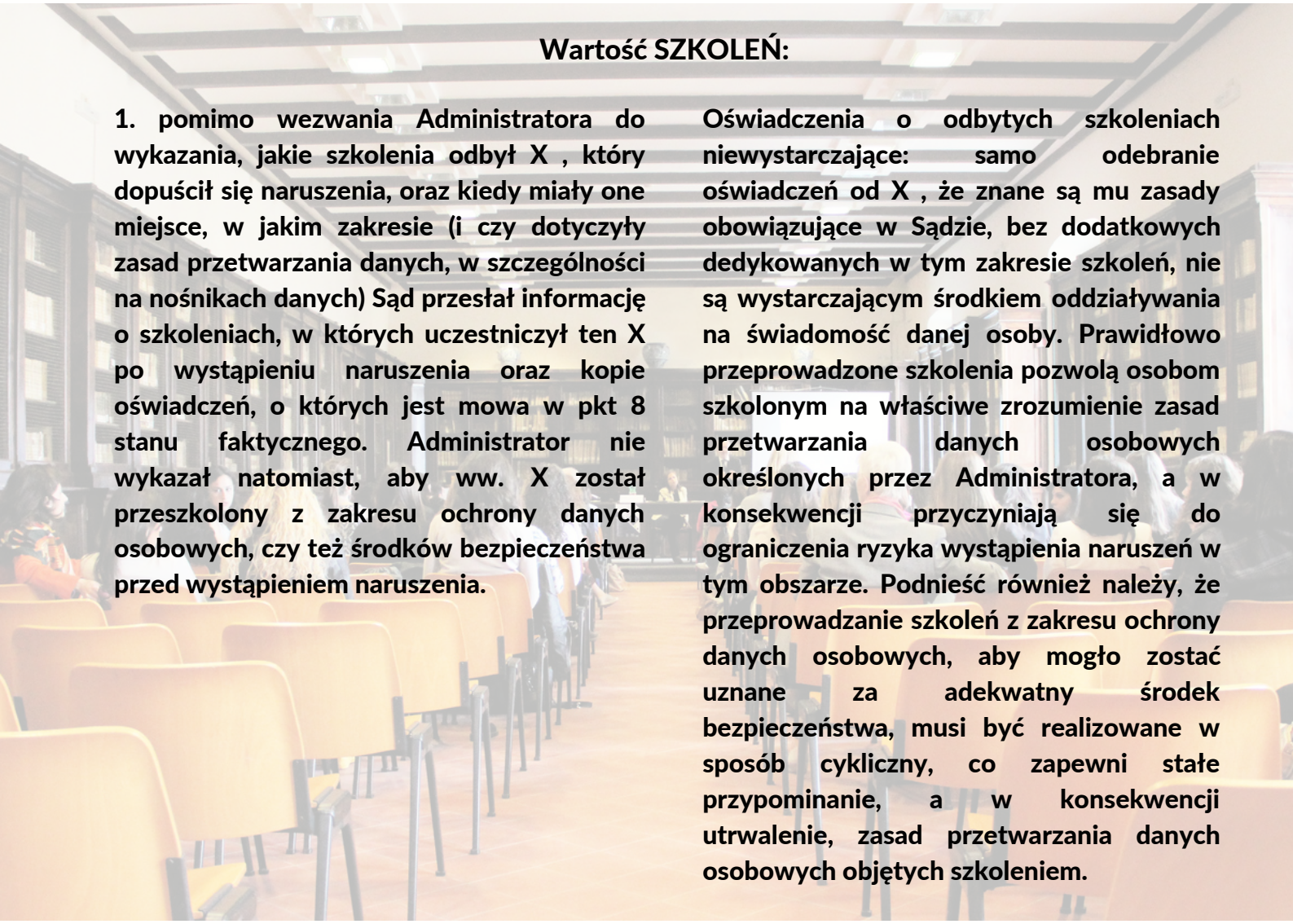
4. Przed naruszeniem: Jakie zabezpieczenia stosował Sąd?
a. w Polityce Ochrony Danych były określone zasady przetwarzania danych osobowych przy użyciu pamięci przenośnych pendrive;
b. pracownicy byli wyposażani w służbowe nośniki danych typu pendrive, na których stosowano szyfrowanie sprzętowe;
c. korzystanie z prywatnych nośników pamięci było przez Sąd formalnie zabronione;
d. przeprowadzona została Analiza Ryzyka, z której wynikało zagrożenie utraty poufności danych poprzez „dostęp do danych przez osoby nieupoważnione.
e. przeprowadzane audyty, z których wynikało, że w jednostce nie są poblokowane stacje robocze pod kątem możliwości używania prywatnych (niezarejestrowanych) nośników zewnętrznych. Zalecenia: „zablokować stacje robocze służbowych komputerów stacjonarnych i laptopów pod kątem możliwości podłączenia do nich prywatnych pendrive'ów";

5. Po naruszeniu – jakie zabezpieczenia zaczął stosować Sąd?

a. przeprowadził inwentaryzację służbowych nośników oraz zaczął blokować porty USB poprzez zakupione oprogramowanie - brak jest możliwości podłączenia innych nośników niż nośniki autoryzowane przez Dział IT Sądu;
b. pracownikom zostały wydane zaszyfrowane nośniki pamięci przenośnych, oddział IT Sądu regularnie (co najmniej raz na pół roku) przypomina pracownikom o konieczności przyniesienia wydanego sprzętu służbowego celem instalacji aktualizacji oprogramowania oraz celem przeprowadzenia przeglądu i inwentaryzacji sprzętu;
c. prowadzone są przez Sąd AUDYTY w pomieszczeniach po godzinach pracy Sądu – taki audyt ma na celu sprawdzenie, czy pracownik poprawnie zabezpiecza przetwarzane informacje oraz powierzone aktywa.

II. Co na to PUODO?

Zabezpieczeniem zastosowanym przez Sąd była procedura, która nie dopuszczała możliwości użytkowania prywatnych nośników danych oraz wydanie X służbowego szyfrowanego nośnika danych. Jednakże wdrożenie przez Administratora tych zabezpieczeń, jak pokazuje przedmiotowa sprawa, nie zapobiegło wystąpieniu naruszenia ochrony danych osobowych, a więc nie było skuteczne.



Wartość SZKOLEŃ:

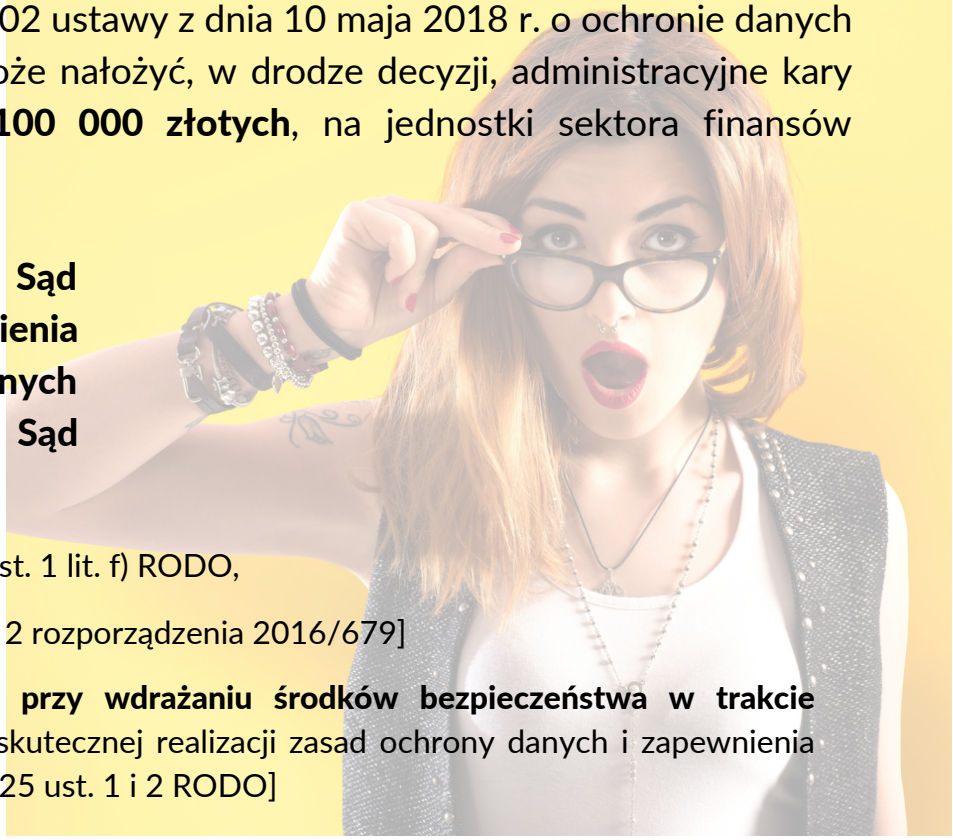
1. pomimo wezwania Administratora do wykazania, jakie szkolenia odbył X , który dopuścił się naruszenia, oraz kiedy miały one miejsce, w jakim zakresie (i czy dotyczyły zasad przetwarzania danych, w szczególności na nośnikach danych) Sąd przesłał informację o szkoleniach, w których uczestniczył ten X po wystąpieniu naruszenia oraz kopie oświadczeń, o których jest mowa w pkt 8 stanu faktycznego. Administrator nie wykazał natomiast, aby ww. X został przeszkolony z zakresu ochrony danych osobowych, czy też środków bezpieczeństwa przed wystąpieniem naruszenia.

Oświadczenia o odbytych szkoleniach niewystarczające: samo odebranie oświadczeń od X , że znane są mu zasady obowiązujące w Sądzie, bez dodatkowych dedykowanych w tym zakresie szkoleń, nie są wystarczającym środkiem oddziaływania na świadomość danej osoby. Prawidłowo przeprowadzone szkolenia pozwolą osobom szkolonym na właściwe zrozumienie zasad przetwarzania danych osobowych określonych przez Administratora, a w konsekwencji przyczyniają się do ograniczenia ryzyka wystąpienia naruszeń w tym obszarze. Podnieść również należy, że przeprowadzanie szkoleń z zakresu ochrony danych osobowych, aby mogło zostać uznane za adekwatny środek bezpieczeństwa, musi być realizowane w sposób cykliczny, co zapewni stałe przypominanie, a w konsekwencji utrwalenie, zasad przetwarzania danych osobowych objętych szkoleniem.

Ponadto, w takich szkoleniach muszą brać udział wszystkie osoby upoważnione do przetwarzania danych osobowych, a samo szkolenie musi obejmować swoim programem wszystkie zagadnienia związane z przetwarzaniem danych osobowych w ramach ustalonego tematu szkolenia. Pominięcie któregoś z tych elementów spowoduje, że szkolenie nie spełni swojej roli, bowiem część osób nie zostanie w ogóle przeszkolona albo uczestnicy szkolenia nie otrzymają pełnej wiedzy w danym zakresie. Konsekwencją powyższego może być naruszenie ochrony danych osobowych, tak jak w sprawie będącej przedmiotem niniejszego postępowania.

III.Kara.

Wysokość kary zależy od ciężaru naruszenia oraz skutków, jakie wynikają z jego popełnienia. Jak stanowi art. 102 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do **100 000 złotych**, na jednostki sektora finansów publicznych.



Pomimo usunięcia przez Sąd uchybień w zakresie zapewnienia bezpieczeństwa przetwarzanych danych, PUODO nałożył na Sąd karę pieniężnej za naruszenie:

1.**zasady poufności danych** [art. 5 ust. 1 lit. f) RODO,

2. **zasady rozliczalności** [art. 5 ust. 2 rozporządzenia 2016/679]

3. obowiązków administratora **przy wdrażaniu środków bezpieczeństwa w trakcie przetwarzania danych,** w celu skutecznej realizacji zasad ochrony danych i zapewnienia domyślnej ochrony danych [art. 25 ust. 1 i 2 RODO]

4. obowiązku **regularnego testowania, mierzenia i oceniania skuteczności przyjętych środków technicznych i organizacyjnych** mających zapewnić bezpieczeństwo przetwarzania [art. 32 ust. 1 lit. d) RODO]

5. obowiązku **uwzględnienia ryzyka wiążącego się z przetwarzaniem,** wynikającego z nieuprawnionego dostępu do przetwarzanych danych osobowych [art. 32 ust. 2 RODO].

1.Zgodnie z art. 5 ust. 1 lit. f) RODO: dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

2.Zgodnie z art. 24 ust. 1 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.

3.Zgodnie z art. 32 ust. 2 RODO, administrator oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

IV. Jakie okoliczności mają wpływ na <u>obniżenie</u> wysokości wymierzonej kary na przykładzie naruszenia w Sądzie?

1.dobra współpracą Sądu z organem nadzorczym;
2.w pełnym zakresie zrealizowane przez Sąd zalecenia PUODO dotyczące uzupełnienia powiadomienia osób, których dane dotyczą, o zaistniałym naruszeniu;
3.pdjęcie przez Sąd konkretnych i szybkich działań,;
4.wprowadzenie ewidencjonowania i szyfrowania przenośnych pamięci;
5.zablokowanie portów USB uniemożliwiając korzystanie z prywatnych nośników danych, niezarejestrowanych przez Dział IT.

V. Jakie okoliczności są obciążające przy wymierzeniu wysokości wymierzonej kary na przykładzie naruszenia w Sądzie?

1.Charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody.

SZKODA A KRZYWDA: PUODO wskazał, iż w niniejszej sprawie brak jest dowodów, aby osoby, do danych których dostęp uzyskała osoba lub osoby nieuprawnione, doznały szkody majątkowej. Niemniej jednak już samo naruszenie poufności ich danych stanowi dla nich szkodę niemajątkową (krzywdę); osoby fizyczne, których dane pozyskano w sposób nieuprawniony mogą bowiem co najmniej odczuwać obawę przed utratą kontroli nad swoimi danymi osobowymi, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, dyskryminacją, czy wreszcie przed stratą finansową. Ponadto, publiczne zawiadomienie osób nie gwarantuje, że informacja dotarła do każdej osoby, do której powinna ona dotrzeć. Tym samym mogło dojść do sytuacji, w której osoby objęte naruszeniem, nie dysponując wiedzą o naruszeniu mogły nie podjąć działań mających im zapewnić choćby minimum poczucia bezpieczeństwa, poprzez zwiększenie ostrożności w posługiwaniu się własnymi danymi osobowymi.

2.Umyślny lub nieumyślny charakter naruszenia.

Nieuprawniony dostęp do danych osobowych osób, wobec których były podejmowane działania przez Sąd, stał się możliwy na skutek niedochowania należytej staranności przez Sąd. W ocenie organu nadzorczego stanowi to o nieumyślnym charakterze naruszenia, wynikającym z niedbalstwa Sądu, gdyż Administrator posiadał wiedzę na temat zagrożeń związanych z użytkowaniem prywatnych nośników pamięci i brakiem zablokowania portów USB, o czym jednoznacznie świadczą zalecenia powstałe po przeprowadzeniu ww. audytów, czy po przeprowadzonej analizie ryzyka. Pomimo tej wiedzy Administrator podjął jednak działania mające na celu zapewnienie bezpieczeństwa danych wyłącznie w zakresie środków organizacyjnych, pomijając te o charakterze technicznym.
Na negatywną ocenę zasługuje w szczególności, co należy ponownie podkreślić, fakt, że Sąd wprowadził wyłącznie zakaz używania prywatnych nośników pamięci, ale nie przeprowadził testu pod kątem skuteczności tego zabezpieczenia, w tym nie sprawdził, czy rzeczywiście pracownicy stosują się do tego zakazu.

3.Kategorie danych osobowych, których dotyczyło naruszenie.

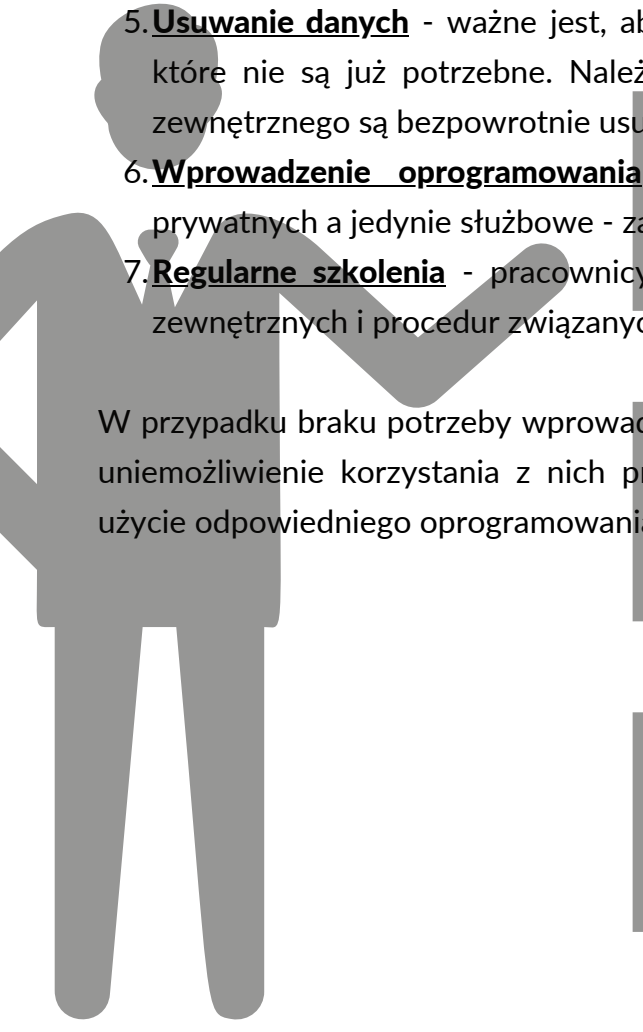
Na zagubionych nośnikach danych znajdowały się projekty orzeczeń, uzasadnień i zarządzeń sporządzone przez X w okresie od grudnia 2004 r. do sierpnia 2020 r. w związku z prowadzonymi przez niego sprawami z zakresu ubezpieczeń społecznych. Oznacza to, że wśród danych mogły znajdować się między innymi też informacje o stanie zdrowia, dane dotyczące przebiegu zatrudnienia, informacji o wynagrodzeniach. Jeżeli zatem znajdowały się tam informacje o stanie zdrowia, to oznacza, że były tam szczególne kategorie danych, które wiążą się z wysokim ryzykiem naruszenia praw lub wolności osób objętych naruszeniem.

Podsumowanie IOD:

Wprowadzenie bezpiecznych procedur dotyczących pracy na dyskach zewnętrznych jest kluczowe dla ochrony danych osobowych. Oto kilka procedur, które mogą pomóc Administratorowi w zapewnieniu bezpieczeństwa przy ich użyciu:

1. **Polityka korzystania z dysków zewnętrznych**, która określa, kto ma uprawnienia do korzystania z dysków zewnętrznych, jakie typy plików mogą być przechowywane na tych dyskach, a także jakich procedury należy przestrzegać podczas korzystania z tych dysków.
2. **Wymuszanie hasła** - należy wymusić użycie hasła do dysku zewnętrznego, aby zapobiec nieuprawnionemu dostępowi do poufnych informacji.
3. **Szyfrowanie** - warto skorzystać z opcji szyfrowania, które są dostępne na wielu dyskach zewnętrznych. Szyfrowanie pomaga zabezpieczyć dane przed nieautoryzowanym dostępem.
4. **Monitorowanie** - należy monitorować korzystanie z dysków zewnętrznych i sprawdzać, czy są używane zgodnie z polityką korzystania z dysków zewnętrznych.
5. **Usuwanie danych** - ważne jest, aby dyski zewnętrzne były regularnie czyszczone z danych, które nie są już potrzebne. Należy również zapewnić, że wszelkie dane usunięte z dysku zewnętrznego są bezpowrotnie usunięte.
6. **Wprowadzenie oprogramowania**, które nie będzie dopuszczało do użytku dysków prywatnych a jedynie służbowe - zaszyfrowane.
7. **Regularne szkolenia** - pracownicy powinni być szkoleni w zakresie korzystania z dysków zewnętrznych i procedur związanych z ich bezpiecznym korzystaniem.

W przypadku braku potrzeby wprowadzania dysków zewnętrznych w pracy zaleca się techniczne uniemożliwienie korzystania z nich przez pracowników poprzez zaślepienie portów USB bądź użycie odpowiedniego oprogramowania.



II. Rozmowa nagrywana – czy interesant może nagrać rozmowę z urzędnikiem bez jego zgody?

W ostatnim czasie wrócił do mnie jak bumerang temat nagrywania rozmów. Zastanawiają Państwa głównie kwestie:

1.Czy interesant może nagrywać bezpośrednią rozmowę z urzędnikiem bez przekazania informacji tym, że rozmowa będzie nagrywana?

2.Czy interesant może nagrywać rozmowy telefoniczne z urzędnikiem?

3.Czy urząd może nagrywać rozmowy telefoniczne?

Odpowiedź IOD:

W przepisach prawa nie znajdziemy zakazu odnośnie nagrywania rozmów z urzędnikiem. Zatem należy stwierdzić, że nie ma ku temu przeszkód.
Czy urzędnik powinien zostać o tym poinformowany i powinien wyrazić na nagrywanie zgodę? Nie widzę podstawy do odmówienie kontynuowania rozmowy przez urzędnika w przypadku wskazania przez petenta, że zamierza nagrywać rozmowę.
W mojej ocenie nie będzie stanowiło to naruszenia jego dóbr osobistych, gdyż rozmowa ta związana będzie z wykonywaniem przez niego funkcji urzędnika a rozmowa prowadzona jest w związku z chęcią uzyskania poszczególnych informacji przez interesanta.

Gmina/Urząd również ma prawo do rejestracji rozmów telefonicznych, a w ich konsekwencji do przetwarzania danych osobowych interesantów (o ile takie dane są niezbędne do osiągnięcia celu rozmowy). Fakt uruchomienia takiego działania realizowany jest w oparciu o przesłankę prawnie uzasadnionych interesów administratora (art. 6 ust. 1 lit. f RODO). Jednakże, sama okoliczność podawania ewentualnych danych przez osoby dzwoniące będzie oparta o przesłankę zgody (art. 6 ust. 1 lit. a RODO) wyrażoną wyraźnym działaniem potwierdzającym - kontynuacja połączenia telefonicznego po wysłuchaniu informacji o nagrywaniu rozmowy.

IIII. Praca zdalna a bezpieczne przetwarzanie danych przez pracowników. Procedury...procedury...procedury!

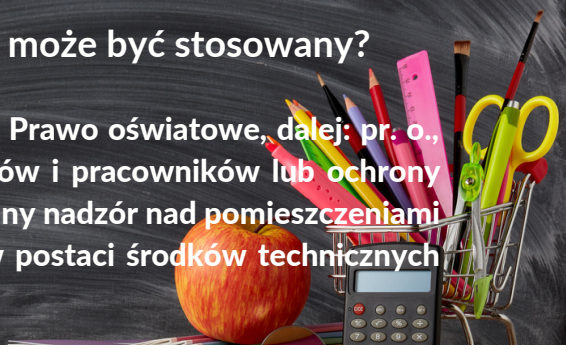
Praca zdalna, czyli możliwość wykonywania obowiązków służbowych poza siedzibą firmy wchodzi w życie z dniem 7 kwietnia 2023 r. Praca będzie mogła być wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (praca zdalna).

Jak wynika z art. 67(26) par. 1-2 Kodeksu pracy (wejście w życie: 7.04.2023 r.), na potrzeby wykonywania pracy zdalnej pracodawca określa procedury ochrony danych osobowych oraz przeprowadza, w miarę potrzeby, instruktaż i szkolenie w tym zakresie. Pracownik wykonujący pracę zdalną potwierdza w postaci papierowej lub elektronicznej zapoznanie się z procedurami oraz jest obowiązany do ich przestrzegania.

Procedury, które wprowadzi pracodawca powinny określać m.in. zasady zabezpieczania sprzętu, dokumentów papierowych, nośników elektronicznych po zakończeniu pracy; postępowania podczas przemieszczania się poza miejscem świadczenia pracy zdalnej wraz z dokumentami, laptopem czy też innymi nośnikami danych; korzystania z urządzeń dostępowych do sieci Internet za pośrednictwem służbowych/ prywatnych urządzeń mobilnych; dostępu do zasobów informatycznych pracodawcy, w tym określenie zasad korzystania z publicznych sieci WiFi; postępowania podczas videokonferencji; prowadzenia korespondencji mailowej; drukowania, kopiowania dokumentów zawierających dane osobowe; udostępniania danych podczas pracy zdalnej; korzystania ze sprzętu do celów prywatnych (o ile jest to przez pracodawcę dozwolone); korzystania z prywatnych urządzeń mobilnych do celów służbowych, *(D. Dörre-Kolasa, Praca zdalna a ochrona danych osobowych, LEX/el. 2023).*

IV. Monitoring w placówkach oświatowych, gdzie nie może być stosowany?

Jak stanowi art. 108a ust. 1 ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe, dalej: pr. o., jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia dyrektor szkoły lub placówki może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).



Monitoring nie powinien stanowić środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły lub placówki (art. 108a ust. 2 pr. o.)

W ustawie wprost uregulowane zostało jakich pomieszczeń monitoring nie może obejmować, tj.: pomieszczeń:

1. w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze;
2. w których uczniom jest udzielana pomoc psychologiczno-pedagogiczna;
3. przeznaczonych do odpoczynku i rekreacji pracowników;
4. pomieszczeń sanitarnohigienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni.

Ustawodawca wskazał jednak, iż jeżeli stosowanie monitoringu w tych pomieszczeniach jest niezbędne ze względu na istniejące zagrożenie dla realizacji celu, dla którego prowadzony jest monitoring, tj.: zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony i nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób – w tych przypadkach Administrator może wprowadzić monitoring również w tych pomieszczeniach.

Widzimy zatem, że powyżej zakaz dotyczący zastosowania monitoringu w w/w pomieszczeniach nie ma charakteru bezwzględnego. Przepis art. 108a ust. 3 pr. o. dopuszcza bowiem instalowanie monitoringu w tych pomieszczeniach, jednak tylko wówczas, jeśli spełnione są jednocześnie następujące warunki:

1. stosowanie monitoringu w wymienionych pomieszczeniach jest niezbędne ze względu na istniejące zagrożenie dla bezpieczeństwa uczniów i pracowników lub ochrony mienia;
2. stosowanie monitoringu w wymienionych pomieszczeniach nie naruszy godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób.

Tylko po spełnieniu wskazanych warunków dopuszczalne jest zainstalowanie monitoringu np. w szatni. Podkreślić trzeba, że stosowany w tych pomieszczeniach monitoring, zgodnie z dyspozycja tego przepisu, nie może rejestrować wizerunku osób, tj. nie może umożliwiać identyfikacji osób przebywających w danym pomieszczeniu. Wobec tego należy rozważyć, czy wymogi związane z instalacją monitoringu np. w szatni (tj. konieczność zastosowania techniki uniemożliwiającej rozpoznanie osób) wpłyną na poprawę bezpieczeństwa. Powyższe dotyczy placówek oświatowych, o których mowa w art. 2 pr. o.

JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/