PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Warszawa, dnia 18 lipca 2023 r.

Decyzja
DKN.5131.47.2022

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775 ze zm.) w związku z art. 7, art. 60 i art. 102 ust. 1 pkt 1 i ust. 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), a także art. 57 ust. 1 lit. a) i h), art. 58 ust. 2 lit. i), art. 83 ust. 1 – 3, art. 83 ust. 4 lit. a) w związku z art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 art. oraz 83 ust. 5 lit. a) w związku z art. 5 ust. 1 lit. f) i art. 5 ust. 2 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 rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35.), po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego w sprawie naruszenia przepisów o ochronie danych osobowych przez K. , Prezes Urzędu Ochrony Danych Osobowych,

stwierdzając naruszenie przez K., przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 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) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), zwanego dalej: „rozporządzeniem 2016/679", polegające na:
1) niezastosowaniu przez K. odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych w przypadku wykonywania pracy przez pracowników zatrudnionych w X. z wykorzystaniem przenośnych komputerów służbowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, co

skutkowało utratą (na skutek kradzieży) przez pracownika X. jego przenośnego komputera wykorzystywanego na potrzeby świadczenia pracy, na którym znajdowały się dokumenty zawierające dane osobowe, które ten pracownik wykorzystywał w celach służbowych,
2) braku regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, w szczególności w związku z wykorzystaniem przenośnych komputerów służbowych, które to naruszenia skutkują naruszeniem zasady „integralności i poufności" (art. 5 ust. 1 lit. f rozporządzenia 2016/679) i rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679),
nakłada na K. za naruszenie przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 administracyjną karę pieniężną w kwocie 15 000 złotych (słownie: piętnastu tysięcy złotych).

Uzasadnienie

K., zwany dalej również K. lub Administratorem, (...) maja 2022 r. dokonał zgłoszenia Prezesowi Urzędu Ochrony Danych Osobowych (zwanemu dalej także „Prezesem UODO") naruszenia ochrony danych osobowych, do którego doszło (...) maja 2022 r. Naruszenie ochrony danych osobowych nastąpiło na skutek włamania do samochodu służbowego osoby zajmującej kierownicze stanowisko i kradzieży jej służbowego komputera przenośnego wykorzystywanego do przetwarzania danych osobowych trzech osób.

W konsekwencji ww. naruszenia ochrony danych osobowych doszło do utraty poufności danych osobowych tych osób. Administrator wskazał, że kategorie danych osobowych, które zostały naruszone, to: nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu oraz numer identyfikacyjny PESEL.

Prezes UODO przeprowadził postępowanie wyjaśniające w sprawie zgłoszonego naruszenia (zarejestrowanego pod sygn. [...]), a następnie wszczął z urzędu w dniu (...) października 2022 r. postępowanie administracyjne w zakresie możliwości naruszenia przez K., jako administratora danych, obowiązków wynikających z przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenie 2016/679.

Prezes UODO, w wyniku przeprowadzonego postępowania wyjaśniającego w sprawie zgłoszonego naruszenia ochrony danych osobowych oraz postępowania administracyjnego ustalił następujący stan faktyczny.

1) Pismem z (...) maja 2022 r., Administrator przekazał organowi nadzorczemu wyjaśnienia, w których

wskazał, że *„(...) skradziony komputer nie posiadał uruchomionej usługi szyfrowania, nie mniej posiadał hasło do konta użytkownika (...)"*. Wskazano ponadto, że na skradzionym komputerze zainstalowano system operacyjny Y., zaznaczając jednocześnie *„(...) obecnie mamy zakupione <klucze> do Z., systemu pozwalającego na uruchomienie B. (...)"*.

2) Administrator w piśmie z (...) czerwca 2022 r. wskazał, że ze skradzionego komputera korzystano poza obszarem przetwarzania danych. Ponadto K. wskazał, że *„(...) sprzęt został ukradziony z samochodu służbowego, którego próbę kradzieży również poczyniono (...)*".

3) Pismem z (...) lipca 2022 r. Prezes UODO zwrócił się do Administratora między innymi o wskazanie, czy została opracowana i wdrożona procedura dotycząca przetwarzania danych osobowych poza siedzibą Administratora, jeśli tak, to czy po naruszeniu ochrony danych osobowych została ona poddana aktualizacji (zwrócono się o przekazanie procedury w wersji obowiązującej przed naruszeniem, jak i po wystąpieniu naruszenia). W odpowiedzi na ww. żądanie, w piśmie z (...) lipca 2022 r. Administrator wskazał, że *„(...) w treści obowiązującej polityki bezpieczeństwa ochrony danych os. funkcjonują zapisy: 1) Wszelkie adnotacje związane z przetwarzaniem danych poza obszarem X., obowiązkowo muszą być przekazywane do IOD nie rzadziej niż co kwartał. Informacja może przekazana zostać drogą elektroniczną, przy zachowaniu formy dokumentu - wzór nr 15 do niniejszej polityki bezpieczeństwa. 2) W przypadku pracy zdalnej [lub telepracy] świadczonej przez osobę będącą pracownikiem X., jako obszar przetwarzania danych w wykazie miejsc przetwarzania danych należy użyć pojęcia zdalna praca lub telepraca na podstawnie umowy o pracę. Powyższe funkcjonowało na zasadach kontaktu telefonicznego, z brakiem zastosowania wzoru dok. nr 15 (załącznik nr 1 do niniejszego pisma), co po naruszeniu ulegnie zmianie. Przetwarzanie poza obszarem będzie bardziej kontrolowane, a stosowanie rejestru w ramach załącznika nr. 15 poddane zostanie audytowi z końcem br. (...)"*. W przedmiocie przeprowadzonych szkoleń pracowników Administrator wyjaśnił, że *„(...) w X. funkcjonuje zasada, iż każdy nowy pracownik zostaje zapoznany z: (...) najistotniejszymi dla pracownika przepisami RODO oraz ustawy o ochronie danych osobowych (...) P. (...) I. (...)"*. Administrator wyjaśnił również, że jest w trakcie aktualizacji oprogramowania *„(...) tak aby wszędzie zaistniała możliwość uruchomienia B. Na chwilę obecną ok. 61 sprzętów mobilnych ma uruchomione szyfrowanie (...)"*. Administrator wskazał ponadto, że planuje do końca 2022 r. wykonać audyt całego sprzętu mobilnego oraz przeprowadzić cykl telekonferencji z pracownikami komórek oraz jednostek organizacyjnych w tematyce bezpieczeństwa ochrony danych osobowych.

4) W odpowiedzi na pytanie organu, czy Administrator odtworzył dane osobowe osób, których dane znajdowały się na skradzionym komputerze przenośnym, Administrator wskazał, że dane osobowe „(...) zostały odtworzone dzięki pamięci przenośnej – dysk zewnętrzny (...)". Wraz z pismem z (...) lipca 2022 r. Administrator przedłożył między innymi „Z. (...)". Szczegółowe zasady dotyczące

wykonywania kopii zapasowej wskazane zostały w załączniku nr 1 do ww. zarządzenia, z którego wynika, że *„(...) celem regularnego wykonywania kopi zapasowej wszystkie jednostki organizacyjne otrzymują po jednym dysku [(...) o pojemności 1 – TB], zabezpieczone hasłem [...] (...) w ramach wykonywania kopi zapasowej, należy uwzględnić wszelkie dane, których utrata mogłaby być dotkliwa w skutkach dla funkcjonowania jednostki, [m.in.: sprawozdania], jak również materiały powiązane z działalnością promocyjną typu: zdjęcia oraz filmy. O randze ważności danych oraz o decyzji wykonania kopii zapasowej, jak również o zakresie danych decyduje Kierownik jednostki organizacyjnej (...) Każda jednostka zobowiązana jest do regularnego wykonywania kopii zapasowej, minimum raz w miesiącu, do 5-tego dnia każdego miesiąca oraz dodatkowo każdorazowo w ramach potrzeb oraz do decyzji kierownika jednostki (...) W ramach weryfikacji prawidłowości wykonywania kopii zapasowych w jednostkach organizacyjnych może nastąpić wyrywkowa kontrola, wykonana przez pracowników B. (...) Każda osoba posiadająca dostęp do dysku, tym samym do danych osobowych na nim zapisanych jest odpowiedzialna za jego bezpieczeństwo. O dostępach pracowników decyduje kierownik jednostki. Co umieszcza na wewnętrznym dokumencie (...)"*. W § 6 dokumentu „Zasady (...)" wskazano, że zgodnie z przyjętą polityką bezpieczeństwa ochrony danych osobowych dyski mogą być używane wyłącznie na terenie jednostki organizacyjnej (ust. 1). Pracownik ma prawo wynieść nośnik poza obszar jednostki organizacyjnej jedynie w przypadku konieczności dostarczenia sprzętu do B., po wcześniejszym zgłoszeniu powyższego do zespołu IT lub IODO (ust. 2). Dysk wraz z protokołem przekazania należy przechowywać w zamykanej szafie, w stosownym pomieszczeniu, do którego nie ma dostępu beneficjent instytucji (ust. 3). Za wyniesienie dysku poza obszar przetwarzania bez uzasadnionego celu oraz zgłoszenia niniejszego faktu do działu zespołu IT lub IODO mogą zostać wyciągnięte konsekwencje służbowe (ust. 4).

5) W odpowiedzi na żądanie organu nadzorczego zawarte w piśmie z (...) lipca 2022 r. o przekazanie analizy ryzyka funkcjonującej przed naruszeniem danych osobowych oraz wykonanej po naruszeniu, Administrator w piśmie z (...) lipca 2022 r. wskazał *„(...) X. przedkłada: 1) Analizę ryzyka przetwarzania danych osobowych poza obszarem przetwarzania dla X. - załącznik nr 3 do niniejszego pisma, wykonaną według metodyki - załącznik nr 4. 2) Tabelę pozwalającą określić wagę naruszenia według metodyki metody oceny wagi naruszenia wg. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), [załącznik nr 5]. (...)".* Załączając egzemplarz analizy ryzyka „KARTA [...] (...)", Administrator nie wskazał w jakiej dacie analiza ryzyka została przeprowadzona.

6) Administrator w piśmie z (...) lipca 2022 r. wyjaśnił ponadto, że *„(...) naruszenie - [kradzież laptopa], dotknęła kierownictwa wyższego, które często wykonuje czynności, z racji swoich obowiązków służbowych, w delegacji. W ramach zaistniałego faktu w znowelizowanej treści polityki bezpieczeństwa danych osobowych w X. dodano stosowne zapisy (...) [zał. 22 do znowelizowanej polityki bezpieczeństwa (...)] (...)"*. W załączniku nr 22 polityki bezpieczeństwa (...) wskazano, że *„(...)*

kierownictwo wyższe X. w sposób szczególny jest zobowiązane do: - sukcesywnego podnoszenia poziomu świadomości w obszarze bezpieczeństwa informacji, w tym ochrony danych osobowych, - regularnemu, [minimum raz na kwartał], poddawaniu pod dyskusję strategii Zarządzania (...), w tym ochrony danych osobowych z IOD oraz ASI, - użytkowania wyłącznie zabezpieczanego, pod kątem ochrony danych, mobilnego sprzętu służbowego, typu: laptop, tablety, telefony. Wszelkie nośniki pamięci użytkowane przez kierownictwo wyższe obowiązkowo muszą posiadać uruchomiony B. Wyjątek może stanowić telefon, pod warunkiem nie przechowywania w nim danych osobowych istotnych dla firmy oraz wiążących się z dużym ryzykiem szkody dla osób których te dane dotyczą (...)".

7) W odpowiedzi na wszczęcie postępowania administracyjnego, pismem z (...) grudnia 2022 r. Administrator poinformował organ nadzorczy, że podjął czynności *„(...) mające na celu rozszerzenie ochrony przed takimi zdarzeniami w przyszłości tj.: wdrożyła uruchomienie B. na komputerach mobilnych typu laptop, posiadających odpowiedni system operacyjny (...) przygotowuje wniosek do jednostki nadrzędnej [...] o wsparcie techniczne, tj. możliwość przekazania lepszej jakości laptopów, które posiadałyby możliwość uruchomienia B. oraz geolokalizacji (...) zaktualizowała polityki bezpieczeństwa [o czym była mowa w piśmie do Prezesa UODO z dnia (...) lipca br.], a dodatkowo poinformowała pracowników X. o zakazie wynoszenia laptopów poza obszar przetwarzania bez wyraźnej zgody Kierownika jednostki oraz Administratora Danych, tj. K. (...) podjęła czynności mające na celu uruchomienie geolokalizacji - planowany czas uruchomienia na wszystkich laptopach posiadających stosowne programowanie to czerwiec 2023 roku (...)"*. Do wyjaśnień załączono oświadczenie pracownika Administratora, zajmującego stanowisko Specjalisty ds. informatyki i telekomunikacji, z (...) października 2022 r., z którego wynika, że w okresie od (...) maja 2022 r. do (...) czerwca 2022 r. *„(...) na urządzeniach elektronicznych typu laptop, należących do X. zostało uruchomione szyfrowanie typu B. (...)"*. Ponadto, wraz z ww. pismem Administrator załączył między innymi: „Analizę nr 1 (...)", „Analizę nr 2 (...)" – Administrator nie wskazał w jakiej dacie ww. analizy ryzyka zostały przeprowadzone.

8) W celu uzyskania jednoznacznych wyjaśnień dotyczących daty przeprowadzonej analizy ryzyka, Prezes UODO ponownie zwrócił się w tej kwestii do Administratora. W piśmie z (...) marca 2023 r. Prezes UODO zwrócił się o: a) wskazanie daty przeprowadzenia analizy ryzyka przed wystąpieniem naruszenia ochrony danych osobowych (dokument ten stanowi załącznik nr 4 do pisma Administratora z (...) grudnia 2022 r.) oraz daty przeprowadzenia analizy ryzyka wykonanej „po uwzględnieniu mechanizmów kontrolnych" (dokument ten stanowi załącznik nr 5 do pisma Administratora z (...) grudnia 2022 r.), b) przesłanie oraz wskazanie daty wykonania analizy ryzyka przeprowadzonej przed dokonaniem analizy ryzyka stanowiącej załącznik nr 4 do pisma Administratora z (...) grudnia 2022 r. (jeżeli taka analiza nie była przeprowadzona, zwrócono się

o wskazanie przyczyny jej niewykonania). W odpowiedzi na ww. pytania organu nadzorczego, Administrator po raz kolejny nie udzielił jednoznacznej odpowiedzi wskazując, w piśmie z (...) marca 2023 r., że *„(...) załącznik nr 4 oraz załącznik nr 3 został przygotowany dodatkowo w formie rozdzielonych analiz w odrębnych plikach na prośbę przedstawicieli GIODO wyrażonej jak zrozumieliśmy podczas wizyty w UODO w dniu (...) października 2022 roku. Obie analizy w oryginalnej wersji były w jednym pliku, który został przedłożony w piśmie z dnia (...).07.2022 r. Plik sam w sobie posiada datę utworzenia zawartości: (...).08.2012 r. [PrtSC - Załącznik nr 1 do niniejszego pisma.]. Powyższe wynika z faktu, iż procesy analiz były prowadzone/tworzone na modyfikowanych plikach po poprzednim pracowniku, który zajmował stanowisko związane z kontrolą wewnętrzną. Pierwsza analiza była wykonywana w okolicach połowy 2020 roku, po czym plik był weryfikowany w czasie zaistnienia naruszenia. Dokonana została zmiana m.in. w sformułowaniu dot. wynoszenie urządzeń mobilnych typu laptop/tablet, zawierających dane os., bez zgody (...) Wcześniej w brzmieniu wynoszenie nośników danych typu laptop [...]. Analiza ryzyka dotyczy czynności i jest plikiem aktywnym (...)”*. Ponadto, w piśmie z (...) marca 2023 r. Administrator wskazał, że *„(...) (...).03.2023 została zakończona procedura wdrażania pakietu usług od firmy M., dzięki czemu korzystając z usługi A. wszystkie komputery zostały zarejestrowane w organizacji. Powyższe pozwala na sprawdzanie aktywności oraz numerów IP logowania konkretnych pracowników, a także monitorowania połączeń Internetowych w przypadku utraty laptopa (...)”*.

Organ nadzorczy dokonał oceny materiału dowodowego pod kątem zbadania jego wiarygodności i mocy dowodowej. Prezes UODO uznał przeważającą większość przedłożonych przez Administratora dowodów za wiarygodne. Za powyższym przemawia fakt, że kluczowe wyjaśnienia Administratora są logiczne, spójne i korelują z całością materiału dowodowego. Nie może jednak umknąć uwadze fakt, iż Administrator przedkładając wyjaśnienia dostarczał dokumenty (dowody na ich potwierdzenie), z których nie wynikało, w jakiej dacie zostały one wytworzone. Powyższe skutkowało koniecznością uzyskiwania przez organ dodatkowych wyjaśnień w celu dokładnego ustalenia i zbadania stanu faktycznego. Powyższe nie oznacza, że Prezes UODO uznał jakikolwiek z kluczowych dla rozstrzygnięcia dowodów za niewiarygodny i nieposiadający mocy dowodowej. Ma to jednak istotny wpływ na ocenę stopnia współpracy Administratora z Prezesem UODO w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków. Szczegółowa analiza poszczególnych dokumentów dostarczonych przez Administratora (w przypadku wystąpienia wątpliwości po stronie organu, co do ich wiarygodności i mocy dowodowej) została przeprowadzona w dalszej części uzasadnienia.

W tym stanie faktycznym, po zapoznaniu się z całością zgromadzonego w sprawie materiału dowodowego, Prezes Urzędu Ochrony Danych Osobowych zważył, co następuje.

Na wstępie należy wskazać, że w przedmiotowej sprawie administratorem danych jest K., bowiem – zgodnie z art. 4 pkt 7) rozporządzenia 2016/679 – „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. (...)

Potwierdzeniem powyższego jest także przedłożony do akt niniejszego postępowania dokument „Polityka (...)". Zgodnie § 3 pkt 5 ww. dokumentu, Administrator Danych Osobowych (ADO) - oznacza K. W ww. dokumencie wskazano między innymi „(...) *§6 OBOWIĄZKI OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH OSOBOWYCH 1. Obowiązki Administratora Danych Osobowych. a. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ADO wdraża odpowiednie środki organizacyjne i techniczne, aby przetwarzanie odbywało się zgodnie z RODO i aby mógł to jednoznacznie wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualnieniom. b. Zgodnie z art. 37 ust. 1 lit. a RODO, ADO wyznacza Inspektora Ochrony Danych (IOD); c. ADO wyznacza Administratora Systemów Informatycznych (ASI), który jest odpowiedzialny za prawidłowe funkcjonowanie systemów informatycznych w X. d. ADO upoważnia osoby wskazane przez kierowników komórek organizacyjnych do przetwarzania danych osobowych. Wzór upoważnienia stanowi załącznik nr 3 do niniejszej Polityki Ochrony. e. ADO pełni rolę kontrolną w zakresie zasad poprawnego przetwarzania danych osobowych zgodnie z wymogami i zaleceniami RODO (...)".* Powyższe jednoznacznie przesądza, że administratorem danych w niniejszej sprawie jest K.

Na marginesie należy wskazać, że Prezes UODO kierując korespondencję do Administratora określił go jako W., ponieważ w ten sposób Administrator wskazał pełną nazwę administratora w formularzu zgłoszenia naruszenia ochrony danych osobowych z (...) maja 2022 r., który został przez niego przesłany do organu nadzorczego. Z uwagi na fakt, że Administrator odbierał korespondencję od Prezesa UODO i udzielał na nią odpowiedzi organowi nadzorczemu, a wskazanej wyżej rozbieżności na żadnym etapie postępowania administracyjnego Administrator nie prostował, należy uznać, że powyżej opisana niezgodność w nazwie administratora nie miała wpływu na przebieg postępowania administracyjnego. Uznając, że w zgłoszeniu naruszenia ochrony danych osobowych z (...) maja 2022 r. wystąpiła oczywista omyłka pisarska, w celu usunięcie jakichkolwiek wątpliwości, organ nadzorczy uściślił kwestię nazwy administratora w przedmiotowej decyzji, wskazując, że administratorem danych jest K.

Zgodnie z art. 34 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781) - zwanej dalej: ustawą z dnia 10 maja 2018 r., Prezes UODO jest organem właściwym w sprawie ochrony danych i organem nadzorczym w rozumieniu rozporządzenia 2016/679. Stosownie do art. 57 ust. 1 lit. a) i h) rozporządzenia 2016/679, bez uszczerbku dla innych zadań określonych na mocy tego rozporządzenia, każdy organ nadzorczy na swoim terytorium monitoruje i egzekwuje stosowanie niniejszego rozporządzenia oraz prowadzi postępowania w sprawie naruszenia niniejszego rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego.

Art. 5 rozporządzenia 2016/679 formułuje zasady dotyczące przetwarzania danych osobowych, które muszą być respektowane przez wszystkich administratorów, tj. podmioty, które samodzielnie lub wspólnie z innymi ustalają cele i sposoby przetwarzania danych osobowych. Zgodnie z art. 5 ust. 1 lit. f) rozporządzenia 2016/679, 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 („poufność i integralność"). Stosownie zaś do art. 5 ust. 2 rozporządzenia 2016/679, administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Konkretyzację zasady poufności, o której mowa w art. 5 ust. 1 lit. f) rozporządzenia 2016/679, stanowią dalsze przepisy tego aktu prawnego. Zgodnie z art. 24 ust. 1 rozporządzenia 2016/679, 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. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

W myśl z art. 25 ust. 1 rozporządzenia 2016/679, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Z treści art. 32 ust. 1 rozporządzenia 2016/679 wynika, że administrator jest zobowiązany do zastosowania środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw

i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Przepis precyzuje, że decydując o środkach technicznych i organizacyjnych należy wziąć pod uwagę stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Z przytoczonego przepisu wynika, że ustalenie odpowiednich środków technicznych i organizacyjnych jest procesem dwuetapowym. W pierwszej kolejności istotnym jest określenie poziomu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych uwzględniając przy tym kryteria wskazane w art. 32 ust. 1 rozporządzenia 2016/679, a następnie należy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Ustalenia te, w stosownym przypadku, powinny obejmować środki takie, jak pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W myśl art. 32 ust. 2 rozporządzenia 2016/679, 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.

Jak wskazuje art. 24 ust. 1 rozporządzenia 2016/679, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze są czynnikami, które administrator ma obowiązek uwzględniać w procesie budowania systemu ochrony danych, również w szczególności z punktu widzenia pozostałych obowiązków wskazanych w art. 25 ust. 1, art. 32 ust. 1 czy art. 32 ust. 2 rozporządzenia 2016/679. Wskazane przepisy uszczegóławiają zasadę poufności określoną w art. 5 ust. 1 lit. f) rozporządzenia 2016/679, a przestrzeganie tej zasady jest konieczne dla prawidłowej realizacji zasady rozliczalności wynikającej z art. 5 ust. 2 rozporządzenia 2016/679.

Jedną z podstaw prawnej ochrony danych osobowych wprowadzoną rozporządzeniem 2016/679 jest obowiązek zapewnienia bezpieczeństwa przetwarzanych danych, określony między innymi w art. 32 ust. 1 rozporządzenia 2016/679. Przepis ten wprowadza podejście oparte na ryzyku, wskazując jednocześnie kryteria, w oparciu o które administrator powinien dokonać wyboru odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Obok ryzyka naruszenia praw lub wolności osób fizycznych należy zatem uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.

Administrator dla prawidłowej realizacji obowiązków wynikających z wyżej przywołanych przepisów rozporządzenia 2016/679 powinien w pierwszej kolejności przeprowadzić analizę ryzyka i na jej podstawie określić i wdrożyć adekwatne środki zapewniające bezpieczeństwo w procesie przetwarzania danych osobowych. W przypadku, gdy Administrator przewidział możliwość używania sprzętu komputerowego (na którym są przetwarzane dane osobowe) poza swoją siedzibą, przedmiotowa analiza powinna wskazywać na ewentualne ryzyka wynikające z możliwości jego wykorzystywania w związku ze świadczeniem pracy poza siedzibą organizacji. Konsekwentnie, przedmiotowa analiza powinna przewidywać właściwe środki bezpieczeństwa w celu minimalizacji ryzyka wystąpienia naruszenia ochrony danych osobowych.

W realiach niniejszej sprawy wskazać należy, że Administrator dopuszczając możliwość przetwarzania danych osobowych przy użyciu przenośnych komputerów służbowych poza siedzibą jego organizacji, w oparciu o właściwie przeprowadzoną analizę ryzyka, winien zidentyfikować zagrożenia dla przetwarzanych w ten sposób danych osobowych, a następnie określić oraz wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa tych danych, a także regularnie sprawdzać skuteczność tych środków, stosownie do wymogów wynikających z art. 32 ust. 1 i 2 rozporządzenia 2016/679.

W omawianym przypadku przeprowadzenie takiej analizy było szczególnie istotne z uwagi na specyfikę pracy wykonywanej na stanowisku, w którym przewidziano świadczenie pracy w delegacji. Powyżej wskazane okoliczności, z uwagi na konieczność przyjęcia rozwiązań w zakresie przetwarzania danych osobowych, powinny spowodować podjęcie szeregu dodatkowych działań zapewniających bezpieczeństwo danych osobowych, a punktem wyjścia do ich określenia winno być, co ponownie należy podkreślić, przeprowadzenie analizy ryzyka, która zakłada możliwość utraty dostępu (np. w następstwie kradzieży lub zagubienia) do sprzętu komputerowego wykorzystywanego do przetwarzania danych osobowych przez pracowników poza organizacją administratora i w następstwie tego naruszenie poufności danych znajdujących się na tym sprzęcie. Podnieść również należy, że obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu nadania przetwarzaniu niezbędnych zabezpieczeń z uwagi na przyjęty sposób przetwarzania danych osobowych wynika także wprost z art. 25 ust. 1 rozporządzenia 2016/679. Przepis ten nakazuje administratorowi danych uwzględnienie ochrony danych w szczególności w fazie projektowania, co oznacza, że Administrator dając możliwość wykorzystywania przez osoby zatrudnione komputerów przenośnych poza siedzibą organizacji Administratora powinien już na tym etapie określić (i wdrożyć) skuteczne środki bezpieczeństwa.

Rozporządzenie 2016/679 wprowadziło podejście, w którym zarządzanie ryzykiem jest fundamentem działań związanych z ochroną danych osobowych i ma charakter ciągłego procesu.

Podmioty przetwarzające dane osobowe zobligowane są nie tylko do zapewnienia zgodności z wytycznymi ww. rozporządzenia poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Oznacza to, że koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka. Konsekwencją takiej orientacji jest rezygnacja z list wymagań, w zakresie bezpieczeństwa narzuconych przez prawodawcę, na rzecz samodzielnego doboru zabezpieczeń w oparciu o analizę zagrożeń. Administratorom nie wskazuje się konkretnych środków i procedur w zakresie bezpieczeństwa.

W świetle powyższego wskazać należy, że analiza ryzyka przeprowadzana przez administratora danych powinna zostać udokumentowana oraz uzasadniona na podstawie przede wszystkim określenia stanu faktycznego, istniejącego w momencie jej przeprowadzania. Należy wziąć pod uwagę w szczególności charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych. Nie można również w trakcie tego procesu pominąć zakresu oraz charakteru danych osobowych przetwarzanych w toku czynności realizowanych przez administratora danych, albowiem w zależności właśnie od zakresu oraz charakteru ujawnionych danych zależeć będą potencjalne negatywne skutki dla osoby fizycznej w przypadku wystąpienia naruszenia ochrony jej danych osobowych.

Określenie aktywa używane jest dla wskazania wszystkiego, co stanowi wartość dla administratora danych. Pewne aktywa stanowić będą wartość wyższą od innych, i również z tej perspektywy winny być oceniane i zabezpieczane. Bardzo istotne są również wzajemne powiązania występujących aktywów, np. poufność aktywów (danych osobowych) zależna będzie od rodzaju i sposobu przetwarzania tych danych. Ustalenie wartości aktywów jest konieczne do oszacowania skutków ewentualnego incydentu (naruszenia ochrony danych osobowych). Jest oczywistym, że szeroki zakres danych osobowych lub przetwarzanie danych osobowych, o których mowa w art. 9 lub art. 10 rozporządzenia 2016/679, może spowodować (w przypadku wystąpienia naruszenia ochrony danych osobowych) daleko idące negatywne skutki dla osób, których dane dotyczą, więc winny one być oceniane jako aktywa o wysokiej wartości, a co za tym idzie stopień ich ochrony powinien być odpowiednio wysoki.

Określenie istniejących lub stosowanych zabezpieczeń jest konieczne, między innymi w tym celu, aby ich nie powielać. Należy również bezwzględnie sprawdzić skuteczność funkcjonowania tych zabezpieczeń, ponieważ istnienie zabezpieczenia niesprawdzonego po pierwsze może wyeliminować jego wartość, po drugie zaś może dać fałszywe poczucie bezpieczeństwa oraz może skutkować pominięciem (niewykryciem) krytycznej podatności, która wykorzystana spowoduje bardzo negatywne skutki, w tym w szczególności może doprowadzić do naruszenia ochrony danych osobowych.

Podatność jest określana powszechnie jako słabość bądź luka w zabezpieczeniach, która wykorzystana przez dane zagrożenie może zakłócać funkcjonowanie, a także może prowadzić do incydentów bądź naruszeń ochrony danych osobowych. Identyfikowanie zagrożeń polega na określaniu, jakie zagrożenia i z jakiego kierunku (powodu) mogą się pojawić.

Metodą przeprowadzenia analizy ryzyka jest np. zdefiniowanie poziomu ryzyka jako iloczynu prawdopodobieństwa i skutków wystąpienia danego incydentu. Zazwyczaj wykorzystuje się macierz ryzyka, która pozwala zobrazować poziomy ryzyka w sposób wizualny, przedstawiając poziomy ryzyka, dla których organizacja definiuje odpowiednie działania.

Aby analiza ryzyka została przeprowadzona w sposób właściwy, winny być zdefiniowane dla każdego z aktywów zagrożenia, mogące wystąpić w procesach przetwarzania danych. Biorąc pod uwagę w szczególności zakres przetwarzanych danych osobowych przez Administratora przy użyciu skradzionego przenośnego komputera, w celu prawidłowego wywiązania się z obowiązków nałożonych ww. przepisami rozporządzenia 2016/679, Administrator był zobowiązany do podjęcia działań zapewniających właściwy poziom ochrony danych poprzez wdrożenie odpowiednich środków technicznych oraz organizacyjnych, a także działań zmierzających do optymalnego zabezpieczenia i konfiguracji wykorzystywanych zasobów, narzędzi, urządzeń (w tym sprzętu komputerowego) poprzez regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych w postaci testów bezpieczeństwa w zakresie infrastruktury informatycznej oraz aplikacji. Charakter i rodzaj tych działań powinien wynikać z przeprowadzonej analizy ryzyka, w której powinno się zidentyfikować podatności odnoszące się do wykorzystywanych zasobów oraz wynikające z nich zagrożenia, a następnie określić adekwatne środki bezpieczeństwa. W tym tonie wypowiedział się także WSA w Warszawie w wyroku z dnia 13 maja 2021 r., sygn. II SA/Wa 2129/20, gdzie podniósł, że *„Administrator danych powinien zatem przeprowadzić analizę ryzyka i ocenić, z jakimi zagrożeniami ma do czynienia”*.

Podkreślić należy, że zarządzanie ryzykiem (przeprowadzenie analizy ryzyka i na tej podstawie wdrożenie odpowiednich zabezpieczeń) jest jednym z podstawowych elementów systemu ochrony

danych osobowych i, jak wskazuje również powyżej przytoczony wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie, ma charakter ciągłego procesu. Winna więc następować okresowa weryfikacja zarówno adekwatności, jak i skuteczności zastosowanych zabezpieczeń, stosownie do wymogu przewidzianego w art. 32 ust. 1 lit. d) rozporządzenia 2016/679. Administrator danych powinien zatem regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania.

Nowe ryzyka lub zagrożenia mogą zmaterializować się lub zostać ujawnione również samoistnie, w sposób całkowicie niezależny od administratora i jest to fakt, który również powinien być brany pod uwagę zarówno podczas budowania systemu ochrony danych osobowych, jak i w czasie jego realizowania. To zaś z kolei definiuje konieczność prowadzenia regularnej weryfikacji całego systemu ochrony danych osobowych zarówno pod kątem adekwatności, jak i skuteczności wdrożonych rozwiązań organizacyjnych i technicznych, w ramach zarówno przeprowadzanej analizy ryzyka, jak i regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania.

Podkreślić również należy, iż badanie prawdopodobieństwa wystąpienia danego zdarzenia nie powinno opierać się wyłącznie na podstawie częstotliwości występowania zdarzeń w danej organizacji, albowiem fakt nie wystąpienia danego zdarzenia w przeszłości wcale nie oznacza, że nie może ono zaistnieć w przyszłości.

W tym kontekście należy wskazać, że Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19, podniósł, że *„(...) czynności o charakterze techniczno – organizacyjnym leżą w gestii administratora danych osobowych, ale nie mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka oraz charakteru chronionych danych osobowych."*

W przedmiotowej sprawie Administrator był wielokrotnie wzywany przez organ nadzorczy do przedłożenia analizy ryzyka dokonanej przed wystąpieniem naruszenia ochrony danych osobowych, jak i tej dokonanej po jego wystąpieniu. W odpowiedzi na pismo organu nadzorczego z (...) lipca 2022 r., w którym Prezes UODO wniósł o przekazanie analizy ryzyka funkcjonującej przed naruszeniem danych osobowych oraz wykonanej po naruszeniu, Administrator – w piśmie z (...) lipca 2022 r. – dostarczył dokument, z którego nie wynikało, kiedy przedłożona analiza została przez niego przeprowadzona (patrz pkt 5) uzasadnienia faktycznego).

W dostarczonym wraz z ww. pismem pliku zapisanym w formacie .xls o nazwie „Załącznik (...)", w arkuszu o nazwie „Karta (...)", uwzględniono rodzaj przetwarzania danych określony jako

„Przetwarzanie danych osobowych poza obszarem przy wykorzystaniu nośnika danych typu laptop/tablet/dysk zewnętrzny (dane wykluczające art. 9)" oraz „Przetwarzanie danych osobowych poza obszarem przy wykorzystaniu nośnika danych typu laptop/tablet/dysk zewnętrzny (dane uwzględniające art. 9)". W ramach ww. rodzajów przetwarzania – w części „Karty (...)" określonej jako „Ryzyko inherentne" – Administrator zidentyfikował zagrożenia, w tym te, które określił jako „zagubienie/kradzież sprzętu przy braku uruchomionych <narzędzi> szyfrujących" ustalając przy tym poziom ryzyka jako wysoki, jednocześnie wskazując, że: „Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, wymaga stałego monitorowania", a jako „Rekomendacje/Zalecenia/Mechanizmy kontrolne" wskazał: „zabezpieczenie wszystkich mobilnych urządzeń systemami szyfrującymi, np. B.".

W części „Karty (...)" określonej jako „Ryzyko rezydualne (po uwzględnieniu mechanizmów kontrolnych)" Administrator zidentyfikował, tożsame z powyżej opisanymi, rodzaje przetwarzania danych i zagrożenia, z tą różnicą, że – w przypadku kluczowych z punktu widzenia przedmiotowej sprawy zagrożeń, tj. zagubienie/kradzież sprzętu przy braku uruchomionych <narzędzi> szyfrujących – Administrator dokonał korekty poziomu ryzyka wskazując, że jest on niskie, a poziom tego ryzyka jest akceptowalny.

Powyżej omówiona analiza ryzyka została ponownie przekazana organowi nadzorczemu wraz z pismem z (...) grudnia 2022 r. w formie załączników (patrz pkt 7) uzasadnienia faktycznego) z tą różnicą, że została ona przedstawiona w formie dwóch plików zapisanych w formacie .xls. Zarówno w przypadku analizy ryzyka dostarczonej wraz z pismem z (...) lipca 2022 r., jak i w przypadku tej dostarczonej wraz z pismem z (...) grudnia 2022 r. Administrator nie wskazał daty ich przeprowadzania. Ponadto użyte przez Administratora określenia „ryzyko inherentne" i „ryzyko rezydualne" nie umożliwiają dokonanie jednoznacznej oceny tego, czy Administrator przeprowadził analizę ryzyka przed wystąpieniem naruszenia.

Zaznaczyć w tym miejscu należy, że forma przedłożonej analizy jest nieczytelna a niektóre zawarte w niej zapisy są niezrozumiałe. Co prawda, Administrator samodzielnie decyduje o formie i treści przeprowadzonej analizy, ale powinien być on w stanie, zgodnie z zasadą rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679), wykazać, że taka analiza została przeprowadzona właściwie, tzn. stanowi ona odpowiednie narzędzie dla skutecznego wdrożenia, a następnie monitorowania środków gwarantujących bezpieczeństwo w procesie przetwarzania danych osobowych. Przede wszystkim należy podnieść, że przedstawiona analiza ryzyka nie wskazuje na przyczyny mitygacji – kluczowego w niniejszej sprawie – ryzyka, tzn. z przedłożonej analizy wynika, że Administrator obniżył ryzyko wystąpienia zagrożenia, jakim jest „zagubienie/kradzież sprzętu przy braku uruchomionych <narzędzi> szyfrujących" wskazując, że ryzyko jest akceptowalne (podczas gdy – zgodnie

z poprzednią wersją analizy ryzyka – było ono nieakceptowalne).

Brak wskazania dat przeprowadzenia ww. analiz skłonił organ nadzorczy do skierowania kolejnego pisma z żądaniem wskazania brakujących informacji, niezbędnych do dokładnego i pełnego ustalenia stanu faktycznego. W piśmie z (...) marca 2023 r., Administrator po raz kolejnych udzielił wymijających odpowiedzi, ograniczając się do stwierdzenia, że *„(...) pierwsza analiza była wykonywana w okolicach połowy 2020 roku, po czym plik był weryfikowany w czasie zaistnienia naruszenia. Dokonana została zmiana m.in. w sformułowaniu dot. wynoszenie urządzeń mobilnych typu laptop/tablet, zawierających dane os., bez zgody O. (...)"*.

Wskazać ponadto należy, że Prezes UODO nie uznał wiarygodności dowodu: „Załącznik nr 1 – PrtSC Szczegółów utworzenia pliku", który został doręczony przez Administratora wraz pismem z (...) marca 2023 r. W opinii Administratora z ww. załącznika miałoby wynikać, że *„(...) obie analizy w oryginalnej wersji były w jednym pliku, który został przedłożony w piśmie z dnia (...).07.2022 r. Plik sam w sobie posiada datę utworzenia zawartości: (...).08.2012 (...)*". Informacja zawarta we właściwościach pliku zapisanym w formacie .xls, o aktualnej nazwie „Załącznik (...)", o tym, że plik ten został utworzony (...) sierpnia 2012 r. nie dowodzi tego, że sama analiza ryzyka została w tym dniu utworzona. Zawartość pliku w formacie .xls o aktualnej nazwie „Załącznik (...)" mogła ulegać wielokrotnej zmianie (tzn. rzeczony plik mógł zawierać dowolną zawartość pod warunkiem, że zapisanie tych danych mogło zostać dokonane w formacie .xls), co więcej sama nazwa tego pliku również mogła być wielokrotnie zmieniana. Wobec powyższego, załączony zrzut z ekranu wskazujący na właściwości pliku o formacie .xls o aktualnej nazwie „Załącznik (...)" nie posiada żadnej wartości dowodowej. Co więcej, biorąc pod uwagę ciągłe unikanie przez Administratora udzielenia jednoznacznej odpowiedzi, kiedy faktycznie analiza ryzyka została przeprowadzona, dostarczanie tego typu „dowodów" wskazuje jedynie na brak dobrej współpracy Administratora z organem nadzorczym.

Niezależenie od powyższego, Prezes UODO nie ma jednak podstaw do uznania za niewiarygodne wyjaśnień Administratora, w których wskazuje on, że przeprowadził analizę ryzyka przed wystąpieniem naruszenia. Administrator wyjaśnił, że „(...) pierwsza analiza była wykonywana w okolicach połowy 2020 roku, po czym plik był weryfikowany w czasie zaistnienia naruszenia (...)". Z przedłożonej analizy ryzyka jednoznacznie wynika, że przed wystąpieniem naruszenia Administrator zidentyfikował zagrożenie, które ostatecznie się zmaterializowało i stanowi bezpośrednią przyczynę wystąpienia naruszenia ochrony danych osobowych. Ponadto, sam Administrator zdefiniował również poziom tego ryzyka, wskazał, że jest ono nieakceptowalne („Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, wymaga stałego monitorowania") oraz określił „Rekomendacje / Zalecenia / Mechanizmy kontrolne" wskazując, że należy wdrożyć „zabezpieczenie wszystkich mobilnych urządzeń systemami szyfrującymi, np. B.".

Jak już wyżej wskazano, w stanie faktycznym przedmiotowej sprawy, ryzyko dotyczyło zagrożenia związanego z kradzieżą przenośnego sprzętu komputerowego wykorzystywanego w celach służbowych poza siedzibą organizacji Administratora. Jak ustalono, ww. komputer był zabezpieczony przed nieautoryzowanym dostępem jedynie za pomocą hasła. W tym miejscu wskazać należy, że w odniesieniu do komputerów przenośnych wynoszonych poza organizację Administratora, z uwagi na zagrożenia z tym związane, w celu przeciwdziałania potencjalnym skutkom naruszenia i zapobieżenia utracie poufności danych osobowych znajdujących się na takim urządzeniu, administrator, stosownie do ww. przepisów rozporządzenia 2016/679, zobowiązany jest zastosować dodatkowe zabezpieczenia w postaci np. szyfrowania dysków twardych komputera. Określenie tych dodatkowych zabezpieczeń powinno nastąpić w wyniku przeprowadzonej analizy ryzyka, po prawidłowej identyfikacji zagrożeń dla danych osobowych przetwarzanych przy użyciu komputerów przenośnych użytkowanych poza organizacją Administratora.

Jak wynika z przedstawionej przez Administratora analizy ryzyka przeprowadzonej (jak sam twierdzi) przed wystąpieniem naruszenia, Administrator miał świadomość ryzyk związanych z utratą sprzętu komputerowego wynoszonego poza jego organizację (szczegółowo kwestię tę omówiono już powyżej). Jeszcze raz należy podkreślić, że Administrator ocenił to ryzyko jako nieakceptowalne i określił, w ramach sposobu postępowania z ryzykiem, zabezpieczenia, jakie należy wdrożyć w celu jego ograniczenia. Wśród wymienionych zabezpieczeń mających obniżyć poziom ryzyka Administrator wskazał, że należy wdrożyć „zabezpieczenie wszystkich mobilnych urządzeń systemami szyfrującymi, np. B". Podkreślić należy, że obowiązek wprowadzenia szyfrowania nośników danych wynika także z art. 32 ust. 1 lit. a) rozporządzenia 2016/679.

W ocenie Prezesa UODO, od momentu opracowania analizy ryzyka (tj. – jak wyjaśnia sam Administrator – od „połowy 2020 r.") do dnia stwierdzenia naruszenia ochrony danych osobowych (naruszenie zostało stwierdzone [...] maja 2022 r.) minęło wystarczająco dużo czasu dla wdrożenia mechanizmów mitygujących – nieakceptowalny przez samego Administratora – poziom ryzyka dla operacji związanych z przetwarzaniem danych osobowych poza siedzibą organizacji Administratora przy wykorzystaniu nośnika danych typu laptop / tablet / dysk zewnętrzny w związku z możliwością zagubienia lub kradzieży sprzętu przy „braku uruchomionych <narzędzi> szyfrujących".

Administrator, pomimo, że w analizie ryzyka (przeprowadzonej w 2020 r.) prawidłowo zidentyfikował zagrożenia dla danych osobowych przetwarzanych przy użyciu komputerów wynoszonych poza jego organizację, a także prawidłowo określił poziom ryzyka dla ww. danych oraz zdefiniował sposób postępowania z ryzykiem poprzez wskazanie zabezpieczeń, które należy zastosować dla obniżenia tego ryzyka, nie podjął żadnych działań, aby rzeczywiście to ryzyko wyeliminować lub ograniczyć do poziomu akceptowalnego. Efektem braku działania Administratora w tym zakresie była materializacja

zidentyfikowanego zagrożenia w postaci kradzieży służbowego komputera z danymi osobowymi, na którym nie zastosowano odpowiednich zabezpieczeń w celu ochrony tych danych, co skutkowało naruszeniem ich poufności.

Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w uzasadnieniu wyroku z 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19, *„Przepis ten* [art. 32 rozporządzenia 2016/679] *nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością."*, a także *„Przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka."*

Administrator pomimo wezwania organu nadzorczego do wskazania, czy została opracowana i wdrożona procedura dotycząca przetwarzania danych osobowych poza siedzibą administratora, a jeżeli tak, to czy po naruszeniu ochrony danych osobowych została ona poddana aktualizacji (zwrócono się o przekazanie procedury w wersji obowiązującej przed naruszeniem, jak i po wystąpieniu naruszenia), ograniczył się do przesłania znowelizowanej „Polityki (...)". Wobec tego, Prezes UODO – mimo podjęcia próby uzyskania wyjaśnień w celu ustalenia szczegółowych zasad, jakie Administrator określił w przypadku dopuszczenia przez niego przetwarzania danych osobowych poza siedzibą jego organizacji – nie był w stanie ocenić, czy Administrator zastosował się do własnych procedur w tym zakresie. Brak możliwości przeprowadzenia takiej oceny ma jednak znaczenie drugorzędne, w tym sensie, że Administrator nie przedkładając dokumentu regulującego kwestię przetwarzania danych osobowych przy wykorzystaniu przenośnego sprzętu komputerowego poza siedzibą jego organizacji, nie wykazał – zgodnie za zasadą rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679) – by określone przez niego zasady (obowiązujące przed wystąpieniem naruszenia ochrony danych osobowych) zakładały wdrożenie odpowiednich środków technicznych w czasie przetwarzania danych osobowych, aby przetwarzanie to odbywało się zgodnie z rozporządzeniem 2016/679. W konsekwencji Prezes UODO nie jest w stanie ocenić, czy i w jaki sposób Administrator dokonywał regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania przed wystąpieniem naruszenia ochrony danych osobowych, a więc czy wywiązał się z obowiązku wynikającego z art. 32 ust. 1 lit. d) rozporządzenia 2016/679.

W orzecznictwie wskazuje się, że *„(...) rozporządzenie 2016/679 nie przesądza jednak o tym, jak*

administrator powinien realizować obowiązki wynikające z zasady rozliczalności zawartej w art. 5 ust. 2 ww. rozporządzenia, niemniej jednak wskazuje na konieczność rozliczania się z przestrzegania przepisów, raportowania ich realizacji oraz przedstawiania dowodów świadczących o prawidłowym wykonywaniu obowiązków. Zasada rozliczalności zobowiązuje administratorów do demonstrowania podjęcia wszelkich środków mających na celu zapewnienie zgodności z obowiązkiem ochrony danych osobowych. W świetle ww. zasady to administrator, a nie organ nadzorczy zajmujący się ochroną danych osobowych, odpowiada za opracowanie, aktualizowanie i utrzymywanie wszystkich procedur i dokumentów związanych z ochroną danych osobowych, a także za stworzenie możliwości dowodowych wykazujących zgodność przetwarzania z przepisami (...)" (wyrok WSA w Warszawie z 1 lutego 2022 r., sygn. II SA/Wa 2106/21, LEX nr 3392761). Powyższe potwierdza orzeczenie WSA w Warszawie z dnia 10 lutego 2021 r., sygn. II SA/Wa 2378/20: *„Zasada rozliczalności bazuje więc na prawnej odpowiedzialności administratora za właściwe wypełnianie obowiązków i nakłada na niego obowiązek wykazania zarówno przed organem nadzorczym, jak i przed podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych ."* Podobnie kwestię zasady rozliczalności interpretuje WSA w Warszawie w wyroku z dnia 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19: *„Biorąc pod uwagę całość norm rozporządzenia 2016/679, podkreślić należy, że administrator ma znaczną swobodę w zakresie stosowanych zabezpieczeń, jednocześnie jednak ponosi odpowiedzialność za naruszenie przepisów o ochronie danych osobowych. Z zasady rozliczalności wprost wynika, że to administrator danych powinien wykazać, a zatem udowodnić, że przestrzega przepisów określonych w art. 5 ust. 1 rozporządzenia 2016/679 ."*

Podsumowując wskazać ponownie należy, że z okoliczności sprawy wynika, że Administrator przed wystąpieniem naruszenia ochrony danych osobowych – mimo że przepisy rozporządzenia 2016/679 obowiązują od 25 maja 2018 r. – nie wprowadził adekwatnych rozwiązań w celu zapobieżenia możliwości naruszenia zasady poufności danych osobowych (art. 5 ust. 1 lit. f) rozporządzenia 2016/679) na skutek materializacji zagrożeń związanych z wykorzystywaniem przenośnych komputerów poza siedzibą jego organizacji, w tym zagrożeń dotyczących kradzieży takiego sprzętu. W konsekwencji, Administrator nie wykazał również przestrzegania w tym zakresie zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679).

Z przedłożonych przez Administratora wyjaśnień wynika, że wdrożenie odpowiednich procedur i rozwiązań nastąpiło dopiero po wystąpieniu przedmiotowego naruszenia ochrony danych osobowych (patrz pkt 7) uzasadnienia faktycznego).

Wskazać należy, że w ww. kwestii wypowiedział się również Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z dnia 19 stycznia 2021 r., sygn. II SA/Wa 702/20, podniósł, że *„(...) administrator danych powinien odpowiednio zabezpieczyć dane osobowe przed ich przypadkową*

utratą za pomocą odpowiednich środków technicznych i organizacyjnych. Dane osobowe powinny być bowiem przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu (motyw 39 rozporządzenia 2016/679)".

Wobec braku zastosowania przez administratora danych adekwatnych środków technicznych mających na celu zminimalizowanie ryzyka naruszenia bezpieczeństwa danych przetwarzanych z wykorzystaniem komputera przenośnego wynoszonego poza organizację Administratora stwierdzić należy, że Administrator nie zapewnił odpowiedniego poziomu zabezpieczenia danych przetwarzanych przy jego użyciu. Przesądza to o niewdrożeniu przez administratora odpowiednich środków technicznych w czasie przetwarzania danych osobowych, aby przetwarzanie to odbywało się zgodnie z rozporządzeniem 2016/679 i w celu nadania przetwarzaniu niezbędnych zabezpieczeń, do czego był on zobowiązany zgodnie z art. 24 ust. 1 i 25 ust. 1 rozporządzenia 2016/679, jak również o niezastosowaniu środków technicznych zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych poprzez zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, do czego zobowiązuje administratora danych art. 32 ust. 1 lit. b) rozporządzenia 2016/679, oraz przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem danych osobowych, o którym mowa w art. 32 ust. 2 rozporządzenia 2016/679, a w konsekwencji również o naruszeniu zasady poufności wyrażonej w art. 5 ust. 1 lit. f) rozporządzenia 2016/679, której ww. przepisy są uszczegółowieniem. Następstwem zaś naruszenia przez Administratora zasady poufności jest naruszenie zasady rozliczalności, o której mowa w art. 5 ust. 2 rozporządzenia 2016/679.

Na podstawie art. 58 ust. 2 lit. i) rozporządzenia 2016/679, każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych przewidzianych w art. 58 ust. 2 lit. a) - h) oraz lit. j) tego rozporządzenia, administracyjnej kary pieniężnej na mocy art. 83 rozporządzenia 2016/679, zależnie od okoliczności konkretnej sprawy. Mając na uwadze ustalenia stanu faktycznego, Prezes Urzędu Ochrony Danych Osobowych, korzystając z przysługującego mu uprawnienia określonego we wskazanym wyżej przepisie rozporządzenia 2016/679 stwierdził, że w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na K. administracyjnej kary pieniężnej.

Zgodnie z art. 83 ust. 4 lit. a) rozporządzenia 2016/679, naruszenia przepisów dotyczących obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 -39 oraz 42 i 43 podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 % jego całkowitego rocznego światowego obrotu

z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Zgodnie z art. 83 ust. 5 lit. a) rozporządzenia 2016/679, naruszenia przepisów dotyczących podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9, podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Art. 83 ust. 3 rozporządzenia 2016/679 natomiast stanowi, że jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

W niniejszej sprawie administracyjna kara pieniężna wobec Administratora nałożona została za naruszenie art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 na podstawie przytoczonego wyżej art. 83 ust. 4 lit. a) rozporządzenia 2016/679, natomiast za naruszenie art. 5 ust. 1 lit. f) i art. 5 ust. 2 rozporządzenia 2016/679 - na podstawie art. 83 ust. 5 lit. a) tego rozporządzenia. Jednocześnie kara nałożona na Administratora łącznie za naruszenie wszystkich powyższych przepisów - stosownie do przepisu art. 83 ust. 3 rozporządzenia 2016/679 - nie przekracza wysokości kary za najpoważniejsze stwierdzone w niniejszej sprawie naruszenie, tj. naruszenie art. 5 ust. 1 lit. f) i art. 5 ust. 2 rozporządzenia 2016/679, które stosownie do art. 83 ust. 5 lit. a) rozporządzenia 2016/679 podlega administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Decydując o nałożeniu administracyjnej kary pieniężnej Prezes UODO - stosownie do treści art. 83 ust. 2 lit. a) - k) rozporządzenia 2016/679 - wziął pod uwagę następujące okoliczności sprawy, stanowiące o konieczności zastosowania w niniejszej sprawie tego rodzaju sankcji oraz wpływające obciążająco na wymiar nałożonej administracyjnej kary pieniężnej:

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** (art. 83 ust. 2 lit. a rozporządzenia 2016/679).
Stwierdzone w niniejszej sprawie naruszenie przepisów ochrony danych osobowych, którego skutkiem była możliwość uzyskania nieuprawnionego dostępu do przetwarzanych przez Administratora danych przez osobę bądź osoby nieuprawnione, a w konsekwencji możliwość

pozyskania danych osobowych osób zatrudnionych w organizacji Administratora, ma znaczną wagę i poważny charakter, stwarza bowiem wysokie ryzyko negatywnych skutków prawnych dla osób, do których danych dostęp mogła mieć osoba bądź osoby nieuprawnione. Naruszenie ochrony danych osobowych dotyczy (...) osób. Naruszenie przez Administratora obowiązków zastosowania środków zabezpieczających przetwarzane dane przed ich udostępnieniem osobom nieupoważnionym, pociąga za sobą nie tylko potencjalną, ale również realną możliwość wykorzystania tych danych przez podmioty trzecie bez wiedzy i wbrew woli osób, których dane dotyczą, niezgodnie z przepisami rozporządzenia 2016/679, np. w celu nawiązania stosunków prawnych lub zaciągnięcia zobowiązań w imieniu osób, których dane pozyskano. (...)

Podkreślić należy również długi czas trwania naruszenia przepisów rozporządzenia 2016/679, bowiem przyjąć należy, iż naruszenie rozpoczęło się w dniu 25 maja 2018 r., tj. w dniu rozpoczęcia stosowania rozporządzenia 2016/679, a zakończyło się (...) czerwca 2022 r. Co prawda, Administrator stwierdził rozpoczęcie naruszenia w dniu (...) maja 2022 r., to jednak Administrator od 25 maja 2018 r. był zobowiązany dostosować procesy przetwarzania danych do wymogów rozporządzenia 2016/679.

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.

2. Nieumyślny charakter naruszenia (art. 83 ust. 2 lit. b rozporządzenia 2016/679).
Administrator był świadomy, w jaki sposób powinien przetwarzać dane osobowe na komputerach przenośnych wydanych pracownikom, aby zapewnić im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, za pomocą odpowiednich środków technicznych i organizacyjnych, a wiec w jaki sposób przestrzegać zasadę „integralności i poufności" wyrażoną w art. 5 ust. 1 li. f) rozporządzenia 2016/679. W przeprowadzonej analizie ryzyka Administrator zidentyfikował prawidłowo zagrożenia i określił poziom ryzyka jako nieakceptowalny. Jednocześnie nie zastosował określonych przez siebie w analizie ryzyka środków bezpieczeństwa, tj. szyfrowania dysków twardych komputerów, a realne działania podjął dopiero po wystąpieniu naruszenia. W działaniach Administratora uwidoczniona została świadomość, co do braku zapewnienia odpowiedniego stopnia bezpieczeństwa danych osobowych przetwarzanych na komputerze przenośnym. Wobec powyższego Administrator był świadomy, że w tym okresie od zidentyfikowania zagrożenia do jego zmaterializowania nie zapewnia odpowiedniego stopnia bezpieczeństwa danych osobowych przetwarzanych na komputerze, co będzie stanowiło naruszenie

przepisów o ochronie danych osobowych. Tym samym, nieumyślnie naruszył przepisy art. 5 ust. 1 li. f) rozporządzenia 2016/679 w zw. z art. 24 ust. 1, 25 ust. 1, 32 ust. 1 i 2 rozporządzenia 2016/679 i w konsekwencji również art. 5 ust. 2 rozporządzenia 2016/679. Biorąc pod uwagę ustalenia w sprawie będącej przedmiotem rozstrzygnięcia niniejszej decyzji należy stwierdzić, że Administrator dopuścił się zaniedbania skutkującego wystąpieniem naruszenia ochrony danych osobowych dotyczącego poufności danych. Tak więc stanowi to istotną okoliczność wpływającą obciążająco na wysokość administracyjnej kary pieniężnej.

3. Kategorie danych osobowych, których dotyczyło naruszenie (art. 83 ust. 2 lit. g rozporządzenia 2016/679).

Dane osobowe znajdujące się na skradzionym komputerze nie należały do szczególnych kategorii danych osobowych, o których mowa w art. 9 rozporządzenia 2016/679, jednakże ich zakres, tj. nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu oraz numer ewidencyjny PESEL, wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych dotkniętych naruszeniem. Należy podkreślić, że w szczególności nieuprawnione ujawnienie takich kategorii danych jak nr ewidencyjny PESEL wraz z imieniem i nazwiskiem, które jednoznacznie identyfikują osobę fizyczną, może realnie i negatywnie wpływać na ochronę praw lub wolności tej osoby. Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 1 lipca 2022 r. sygn. akt II SA/Wa 4143.21 *„W przypadku naruszenia takich danych, jak imię, nazwisko oraz numer PESEL, możliwa jest bowiem kradzież lub sfałszowanie tożsamości skutkująca negatywnymi konsekwencjami dla osób, których dane dotyczą”*. Wskazać należy, że numer ewidencyjny PESEL, czyli jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający m.in. datę urodzenia oraz oznaczenie płci, a więc ściśle powiązany ze sferą prywatną osoby fizycznej oraz podlegający również, jako krajowy numer identyfikacyjny, wyjątkowej ochronie na gruncie art. 87 rozporządzenia 2016/679, jest daną o szczególnym charakterze i takiej szczególnej ochrony wymaga.

4. Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków (art. 83 ust. 2 lit. f) rozporządzenia 2016/679).

Należy w tym miejscu wskazać, że w toku prowadzonego postępowania wyjaśniającego, a następnie postępowania administracyjnego, Administrator nie podjął i nie prowadził dobrej współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków. Prezes UODO zwracał się do Administratora o przedłożenie konkretnych wyjaśnień niezbędnych do ustalenia stanu faktycznego, również w celu ewentualnego skorzystania przez organ nadzorczy z uprawnień przewidzianych w art. 58 ust. 2 lit. d) rozporządzenia 2016/679, tj. uprawnienia do nakazania administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu.

Przykładowo, Prezes UODO pismem z (...) lipca 2022 r. zwrócił się o przekazanie analizy ryzyka funkcjonującej przed naruszeniem danych osobowych oraz wykonanej po naruszeniu. W odpowiedzi na powyższe, organ nadzorczy otrzymał w załączniku do wyjaśnień plik w formacie .xls o nic nie mówiącej nazwie „Załącznik (...)" zawierający dwie analizy (wątpliwości co do rzetelności tych analiz zostały już powyżej omówione) bez wskazania, która z tych analiz została wykonana przed, a która po naruszeniu ochrony danych osobowych. W związku z wątpliwościami organu, co do rzetelności ww. analiz ryzyka, pismem z (...) marca 2023 r. organ ponownie zwrócił się o wskazanie daty przeprowadzenia analizy ryzyka przed wystąpieniem naruszenia ochrony danych osobowych oraz daty przeprowadzenia analizy ryzyka wykonanej „po uwzględnieniu mechanizmów kontrolnych". W odpowiedzi na precyzyjnie zadane pytanie, Administrator przedłożył nieprecyzyjne wyjaśnienia, z których nie możliwości wyciągnięcia jakichkolwiek wniosków, które byłyby istotne dla ustalenia stanu faktycznego przedmiotowej sprawy, poza tymi, które wskazują na to, że Administrator w gruncie rzeczy nie wie kiedy przeprowadził analizę ryzyka, bowiem w piśmie z (...) marca 2023 r. wyjaśnił, że „(...) obie analizy w oryginalnej wersji były w jednym pliku, który został przedłożony w piśmie z dnia (...).07.2022 r. Plik sam w sobie posiada datę utworzenia zawartości: (...).08.2012 r. (...) Pierwsza analiza była wykonywana w okolicach połowy 2020 roku, po czym plik był weryfikowany w czasie zaistnienia naruszenia (...)" (patrz pkt 8 uzasadnienia faktycznego).

Z kolei w odpowiedzi na precyzyjnie sformułowanie żądnie organu o wskazanie, czy została opracowana i wdrożona procedura dotycząca przetwarzania danych osobowych poza siedzibą administratora, jeśli tak, to czy po naruszeniu ochrony danych osobowych została ona poddana aktualizacji (zwrócono się o przekazanie procedury w wersji obowiązującej przed naruszeniem, jak i po wystąpieniu naruszenia), Administrator nie udzielił konkretnej odpowiedzi (patrz pkt 3 uzasadnienia faktycznego), jednocześnie przekazując cały szereg informacji i załączników do pisma z (...) lipca 2012 r., o które organ nie wnioskował. Co więcej, kluczowy z punktu widzenia niniejszego postępowania dokument o nazwie „Polityka (...)" nie został oznaczony datą. Z przedłożonego dokumentu wynika jedynie, że stanowi on „Załącznik nr 1 do Zarządzenia nr ... z dnia czerwca 2022 r." Samego Zarządzenia, którym wprowadzono znowelizowaną politykę bezpieczeństwa, Administrator nie przekazał – jak również nie przekazał stosownego wyjaśnienia, które wskazywałoby na datę ogłoszenia i wprowadzenia przedmiotowego Zarządzenia.

Powyżej opisane działanie Administratora, tj. udzielenie wymijających odpowiedzi na precyzyjnie zadane pytania, niedostarczenie właściwie oznaczonych dokumentów, dostarczanie dokumentów nieistotnych dla rozstrzygnięcia (o przedłożenie których Prezes UODO nie wnioskował), organ nadzorczy ocenia jako celowe działania Administratora mające utrudnić Prezesowi UODO rzetelne przeprowadzenie postępowania administracyjnego, a nade wszystko wydłużyć proces weryfikacji tego, czy stan naruszenia przepisów gwarantujących ochronę danych osobowych nadal się

utrzymuje.

Istotne z punktu widzenia niniejszego postępowania było pozyskanie przez Prezesa UODO od Administratora informacji, które pozwolą na zidentyfikowanie przyczyny wystąpienia naruszenia przepisów o ochronie danych osobowych, ale także na ocenę tego, czy stan naruszenia tych przepisów trwa nadal i czy wobec tego Prezes UODO winien skorzystać z uprawnień naprawczych określonych w art. 58 ust. 2 lit. d) rozporządzenia 2016/679. W tym właśnie celu organ starał się możliwie najbardziej precyzyjnie ustalić ramy czasowe obowiązujących w organizacji Administratora dokumentów i rozwiązań związanych z ochroną danych osobowych, w szczególności analizy ryzyka oraz procedury wykorzystywania w celach służbowych przenośnego sprzętu komputerowego poza siedzibą organizacji Administratora.

W ocenie organu, brak właściwej współpracy Administratora z Prezesem UODO w znaczący sposób przyczynił się do wydłużenia samego postępowania administracyjnego a także procesu naprawczego prowadzonego w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków [art. 83 ust. 2 lit. f) rozporządzenia 2016/679].

Ustalając wysokość administracyjnej kary pieniężnej, Prezes UODO nie stwierdził okoliczności łagodzących, mającą wpływ na obniżenie wysokości wymierzonej kary.

Inne, niżej wskazane okoliczności, o których mowa w art. 83 ust. 2 Rozporządzenia 2016/679, po dokonaniu oceny ich wpływu na stwierdzone w niniejszej sprawie naruszenie, zostały przez Prezesa UODO uznane za neutralne w jego ocenie, to znaczy nie mające ani obciążającego ani łagodzącego wpływu na wymiar orzeczonej administracyjnej kary pieniężnej.

1. Działania podjęte w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą (art. 83 ust. 2 lit. c rozporządzenia 2016/679).
W niniejszej sprawie nie stwierdzono powstania jakiejkolwiek szkody po stronie osób dotkniętych naruszeniem, w związku, z czym Administrator nie był zobowiązany do podjęcia jakichkolwiek działań mających na celu ich zminimalizowanie.

2. Stopień odpowiedzialności administratora z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez niego na mocy art. 25 i 32 (art. 83 ust. 2 lit. d rozporządzenia 2016/679).
W przyjętych w dniu 3 października 2017 r. Wytycznych Grupy Roboczej ds. Ochrony Danych Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 wskazano, że - rozpatrując tę przesłankę - „organ nadzorczy musi odpowiedzieć na

pytanie, w jakim stopniu administrator <zrobił wszystko, czego można by było oczekiwać>, zważywszy na charakter, cele lub zakres przetwarzania oraz w świetle obowiązków nałożonych na niego przez rozporządzenie".

Prezes UODO stwierdził w niniejszej sprawie naruszenie przez Administratora przepisów art. 25 ust. 1, art. 32 ust. 1 i 2 rozporządzenia 2016/679. W jego ocenie na administratorze ciąży w wysokim stopniu odpowiedzialność za niewdrożenie odpowiednich środków technicznych i organizacyjnych, które zapobiegłyby naruszeniu ochrony danych osobowych. Oczywistym jest, że w rozważanym kontekście charakteru, celu i zakresu przetwarzania danych osobowych Administrator nie „zrobił wszystkiego, czego można by było od niego oczekiwać"; nie wywiązał się tym samym z nałożonych na niego przepisami art. 25 i 32 rozporządzenia 2016/679 obowiązków.

W niniejszej sprawie okoliczność ta stanowi jednak o istocie samego naruszenia; nie jest jedynie czynnikiem wpływającym - łagodząco lub obciążająco - na jego ocenę. Z tego też względu brak odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 25 i art. 32 rozporządzenia 2016/679, nie może zostać przez Prezesa UODO uznany w niniejszej sprawie za okoliczność mogącą dodatkowo wpłynąć na surowszą ocenę naruszenia i wymiar nałożonej na K. administracyjnej kary pieniężnej.

3. Wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego (art. 83 ust. 2 lit. e rozporządzenia 2016/679).
Prezes UODO nie stwierdził jakichkolwiek, dokonanych przez Administratora, wcześniejszych naruszeń przepisów o ochronie danych osobowych, w związku z czym brak jest podstaw do traktowania tej okoliczności jako obciążającej. Obowiązkiem każdego administratora jest przestrzeganie przepisów prawa (w tym o ochronie danych osobowych), więc brak wcześniejszych naruszeń nie może być okolicznością łagodzącą przy wymierzaniu sankcji.

4.Sposób w jaki organ nadzorczy dowiedział się o naruszeniu (art. 83 ust. 2 lit. h rozporządzenia 2016/679).
Prezes UODO stwierdził naruszenie w wyniku zgłoszenia naruszenia ochrony danych osobowych dokonanego przez Administratora. Administrator dokonując tego zgłoszenia realizował jedynie ciążący na nim obowiązek prawny, brak jest podstaw do uznania, że okoliczność ta stanowi okoliczność łagodzącą. Zgodnie z *Wytycznymi w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 Wp. 253 „Organ nadzorczy może dowiedzieć się o naruszeniu w wyniku postępowania, skarg, artykułów w prasie, anonimowych wskazówek lub powiadomienia przez administratora danych. Zgodnie z rozporządzeniem administrator ma obowiązek zawiadomić organ nadzorczy o naruszeniu ochrony danych osobowych. Zwykłe*

dopełnienie tego obowiązku przez administratora nie może być interpretowane jako czynnik osłabiający/łagodzący".

5. Przestrzeganie wcześniej zastosowanych w tej samej sprawie środków, o których mowa w art. 58 ust. 2 rozporządzenia 2016/679 (art. 83 ust. 2 lit. i rozporządzenia 2016/679).
Przed wydaniem niniejszej decyzji Prezes UODO nie stosował w wobec Administratora w rozpatrywanej sprawie żadnych środków wymienionych w art. 58 ust. 2 rozporządzenia 2016/679, w związku z czym administrator nie miał obowiązku podejmowania żadnych działań związanych z ich stosowaniem, a które to działania, poddane ocenie Prezesa UODO, mogłyby mieć obciążający lub łagodzący wpływ na ocenę stwierdzonego naruszenia.

6. Stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 rozporządzenia 2016/679 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 rozporządzenia 2016/679 (art. 83 ust. 2 lit. j rozporządzenia 2016/679).
Administrator nie stosuje zatwierdzonych kodeksów postępowania ani zatwierdzonych mechanizmów certyfikacji, o których mowa w przepisach rozporządzenia 2016/679. Ich przyjęcie, wdrożenie i stosowanie nie jest jednak - jak stanowią przepisy rozporządzenia 2016/679 - obowiązkowe dla administratorów i podmiotów przetwarzających w związku, z czym okoliczność ich niestosowania nie może być w niniejszej sprawie poczytana na niekorzyść Administratora. Na korzyść Administratora natomiast mogłaby być uwzględniona okoliczność przyjęcia i stosowania tego rodzaju instrumentów, jako środków gwarantujących wyższy niż standardowy poziom ochrony przetwarzanych danych osobowych.

7. Osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty (art. 83 ust. 2 lit. k rozporządzenia 2016/679).
Prezes UODO nie stwierdził, żeby administrator w związku z naruszeniem odniósł jakiekolwiek korzyści finansowe lub uniknął tego rodzaju strat. Brak jest więc podstaw do traktowania tej okoliczności jako obciążającej administratora. Stwierdzenie zaistnienia wymiernych korzyści finansowych wynikających z naruszenia przepisów rozporządzenia 2016/679 należałoby ocenić zdecydowanie negatywnie. Natomiast nieosiągnięcie przez administratora takich korzyści, jako stan naturalny, niezależny od naruszenia i jego skutków, jest okolicznością, która z istoty rzeczy nie może być łagodzącą dla Administratora. Potwierdza to samo sformułowanie przepisu art. 83 ust. 2 lit. k) rozporządzenia 2016/679, który nakazuje organowi nadzorczemu zwrócić należytą uwagę na korzyści „osiągnięte" - zaistniałe po stronie podmiotu dokonującego naruszenia.

8. Inne obciążające lub łagodzące czynniki (art. 83 ust. 2 lit. k) Rozporządzenia 2016/679).
Prezes UODO wszechstronnie rozpatrując sprawę nie odnotował innych niż opisane powyżej

okoliczności mogących mieć wpływ na ocenę naruszenia i na wysokość orzeczonej administracyjnej kary pieniężnej.

Uwzględniając wszystkie omówione wyżej okoliczności, Prezes Urzędu Ochrony Danych Osobowych uznał, iż nałożenie administracyjnej kary pieniężnej na Administratora jest konieczne i uzasadnione wagą, charakterem oraz zakresem zarzucanych Administratorowi naruszeń. Stwierdzić należy, iż zastosowanie wobec Administratora jakiegokolwiek innego środka naprawczego przewidzianego w art. 58 ust. 2 rozporządzenia 2016/679, w szczególności zaś poprzestanie na upomnieniu (art. 58 ust. 2 lit. b) rozporządzenia 2016/679), nie byłoby proporcjonalne do stwierdzonych nieprawidłowości w procesie przetwarzania danych osobowych oraz nie gwarantowałoby tego, że Administrator w przyszłości nie dopuści się kolejnych zaniedbań.

Odnosząc się do wysokości wymierzonej K. administracyjnej kary pieniężnej wskazać należy, iż w ustalonych okolicznościach niniejszej sprawy – tj. wobec stwierdzenia naruszenia kilku przepisów rozporządzenia 2016/679, tj. zasady poufności danych, wyrażonej w art. 5 ust. 1 lit. f) rozporządzenia 2016/679, a odzwierciedlonej w postaci obowiązków określonych w art. 25 ust. 1, art. 32 ust. 1, art. 32 ust. 2 rozporządzenia 2016/679, a w konsekwencji również art. 5 ust. 2 rozporządzenia 2016/679 (zasady rozliczalności) oraz faktu, iż Administrator jest organem jednostki sektora finansów publicznych – zastosowanie znajdzie art. 102 z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), z którego wynika ograniczenie wysokości (do 100.000 zł) administracyjnej kary pieniężnej, jaka może zostać nałożona na jednostkę sektora finansów publicznych.

W ocenie Prezesa UODO, zastosowana administracyjna kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy funkcje, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679, tzn. będzie w tym indywidulanym przypadku skuteczna, proporcjonalna i odstraszająca.

Zdaniem Prezesa UODO nałożona na Administratora kara będzie skuteczna, albowiem doprowadzi do stanu, w którym Administrator stosował będzie takie środki techniczne i organizacyjne, które zapewnią przetwarzanym danym stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane dotyczą oraz wadze zagrożeń towarzyszącym procesom przetwarzania tych danych osobowych. Skuteczność kary równoważna jest zatem gwarancji tego, iż Administrator od momentu zakończenia niniejszego postępowania będzie z najwyższa starannością podchodzić do wymogów stawianych przez przepisy o ochronie danych osobowych.

Zastosowana administracyjna kara pieniężna jest również proporcjonalna do stwierdzonego naruszenia, w tym zwłaszcza jego wagi, skutku, kręgu dotkniętych nim osób fizycznych oraz wysokiego ryzyka negatywnych konsekwencji, jakie w związku z naruszeniem mogą ponieść. Zdaniem

Prezesa UODO, nałożona na K. administracyjna kara pieniężna nie będzie stanowiła nadmiernego dla niego obciążenia. Wysokość kary została bowiem określona na takim poziomie, aby z jednej strony stanowiła adekwatną reakcję organu nadzorczego na stopień naruszenia obowiązków Administratora, z drugiej jednak strony nie powodowała sytuacji, w której konieczność jej uiszczenia pociągnie za sobą negatywne następstwa, w postaci istotnego pogorszenia sytuacji finansowej Administratora. Zdaniem Prezesa UODO, Administrator powinien i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, stąd nałożenie kary w wysokości 15 000 złotych (piętnastu tysięcy złotych) jest w pełni uzasadnione.

W ocenie Prezesa UODO, administracyjna kara pieniężna spełni w tych konkretnych okolicznościach funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Administratora przepisów rozporządzenia 2016/679, ale i prewencyjną, bowiem przyczyni się do zapobiegania w przyszłości naruszeniom obowiązków Administratora wynikających z przepisów o ochronie danych osobowych.

W ocenie Prezesa UODO, zastosowana kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy przesłanki, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679, ze względu na wagę stwierdzonych naruszeń w kontekście podstawowych wymogów i zasad rozporządzenia 2016/679 - zwłaszcza zasady poufności wyrażonej w art. 5 ust. 1 lit. f) rozporządzenia 2016/679.

Celem nałożonej kary jest doprowadzenie do przestrzegania przez Administratora w przyszłości przepisów rozporządzenia 2016/679.

W tym stanie faktycznym i prawnym Prezes Urzędu Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.