PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Warszawa, dnia 13 lipca 2021 r.

DECYZJA

DKN.5131.22.2021

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2021 r. poz. 735), art. 7 ust. 1, art. 60, 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) oraz 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), art. 83 ust. 5 lit. a) w związku z art. 5 ust. 1 lit. f), art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b) i d) oraz art. 32 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 rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, 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 przetwarzania danych osobowych przez Prezesa Sądu Rejonowego w Zgierzu (Zgierz, ul. Sokołowska 6), Prezes Urzędu Ochrony Danych Osobowych

stwierdzając naruszenie przez Prezesa Sądu Rejonowego w Zgierzu przepisów art. 5 ust. 1 lit. f), art. 24 ust. 1 art. 25 ust. 1, art. 32 ust. 1 lit. b) i d) oraz art. 32 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 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) (dalej jako: rozporządzenie 2016/679), polegające na niewdrożeniu przez Prezesa Sądu Rejonowego w Zgierzu odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu przenośnych pamięci zewnętrznych, zapewniających bezpieczeństwo zapisanych tam danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem

oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, co skutkowało utratą przenośnej pamięci zewnętrznej z danymi osobowymi, zapisanymi na niej w sposób niezabezpieczony, nakłada na Prezesa Sądu Rejonowego w Zgierzu za naruszenie art. 5 ust. 1 lit. f), art. 25 ust. 1, art. 32 ust. 1 lit. b) i d) oraz art. 32 ust. 2 rozporządzenia 2016/679 administracyjną karę pieniężną w kwocie 10 000 PLN (słownie: dziesięć tysięcy zł).

UZASADNIENIE

Do Urzędu Ochrony Danych Osobowych [...] lutego 2020 r. wpłynęło zgłoszenie naruszenia ochrony danych osobowych podpisane przez Prezesa Sądu Rejonowego w Zgierzu (dalej jako: Prezes Sądu lub administrator), zarejestrowane pod sygnaturą [...], informujące o naruszeniu ochrony danych osobowych 400 osób, podlegających nadzorowi kuratorskiemu i objętych wywiadem środowiskowym przez kuratora sądowego, w zakresie imion i nazwisk, dat urodzenia, adresów zamieszkania lub pobytu, numerów ewidencyjnych PESEL, danych dotyczących zarobków i/lub posiadanego majątku, serii i numerów dowodów osobistych, numerów telefonów, danych dotyczących zdrowia oraz danych dotyczących wyroków skazujących. Incydent stanowiący przedmiot zgłoszenia miał miejsce [...] lutego 2020 r. i polegał na zagubieniu nieszyfrowanej przenośnej pamięci zewnętrznej typu pendrive przez kuratora sądowego. W rubryce 2A formularza zgłoszenia jako administrator danych wskazany został Sąd Rejonowy w Zgierzu.

Z uwagi na zakres ujawnionych danych osobowych wskazane naruszenie spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Administrator poinformował zatem, iż w dniu [...] lutego 2020 r. opublikował na stronie internetowej Sądu Rejonowego w Zgierzu, zwanego dalej „Sądem", komunikat o naruszeniu, wskazując, że *„możliwe, że ktoś będzie próbował wykorzystać dane tam zapisane"*. Poprosił również o *„czujność, a w przypadku uzyskania informacji o ewentualnych próbach wykorzystania danych, którymi dysponował Sąd - o niezwłoczne zawiadomienie organów ścigania oraz kontakt z Sądem Rejonowym w Zgierzu"*.

Pismami z dnia [...] maja oraz [...] lipca 2020 r., Prezes Urzędu Ochrony Danych Osobowych (dalej także Prezes Urzędu), wystąpił o ponowne, prawidłowe powiadomienie osób fizycznych, albowiem komunikat skierowany do osób, których dane dotyczą, nie spełniał warunków określonych w rozporządzeniu 2016/679 w zakresie opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Ponadto, pismami z [...] maja i [...] lipca 2020 r. Prezes Urzędu zwrócił się o złożenie dodatkowych wyjaśnień, między innymi:

1. Czy i w jaki sposób rekomendowano kuratorom sądowym zabezpieczanie danych zapisywanych na zewnętrznych nośnikach pamięci.
2. Czy administrator danych osobowych opracował i wdrożył procedury korzystania z zewnętrznych nośników pamięci oraz zabezpieczania danych osobowych, przetwarzanych na nośnikach zewnętrznych poza siedzibą administratora.
3. Czy zagubiony nośnik pamięci został wydany kuratorowi przez administratora, czy też należał do

kuratora.
4. Jeśli zagubiony nośnik był własnością kuratora, czy procedury administratora danych dopuszczają taką możliwość oraz w jaki sposób sprawowana jest kontrola nad takim przetwarzaniem danych osobowych.

W odpowiedzi na wystąpienie, w dniu [...] sierpnia 2020 r. Administrator poinformował o zamieszczeniu uzupełnionego komunikatu o naruszeniu ochrony danych osobowych, zaś pismem z [...] sierpnia 2020 r. wskazał, iż:

1. Kuratorom rekomendowano stosowanie się do regulaminu ochrony danych w Sądzie oraz procedur ochrony danych w rozmowach indywidualnych oraz podczas spotkań szkoleniowych.
2. Opracował i wdrożył procedury korzystania z zewnętrznych nośników pamięci oraz zabezpieczenia danych osobowych przetwarzanych na nośnikach zewnętrznych poza swoją siedzibą, zaś procedura ta jest częścią Instrukcji Zarządzania Systemem Informatycznym w Sądzie Rejonowym w Zgierzu.
3. Zagubiony nośnik pamięci został wydany kuratorowi przez Sąd, natomiast Regulamin ochrony danych dla Sądu zabrania korzystania z prywatnych nośników danych dla przetwarzania danych służbowych.

W związku z przedstawionymi wyjaśnieniami, pismem z dnia [...] września 2020 r. Prezes Urzędu wszczął z urzędu postępowanie administracyjne, wobec możliwości naruszenia przez Sąd Rejonowy w Zgierzu, jako administratora danych, obowiązków wynikających z rozporządzenia 2016/679, tj. art. 5 ust. 1 lit. f), art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2, w związku z naruszeniem ochrony danych osobowych (sygn. [...]). Ponadto, Prezes Urzędu wezwał Sąd do przedstawienia kolejnych wyjaśnień oraz dokumentacji dotyczących:

1. Wskazania, czy przed wystąpieniem przedmiotowego naruszenia, administrator danych określił zasady przetwarzania danych osobowych oraz stosowane zabezpieczenia przy użyciu pamięci przenośnych pendrive, a jeśli tak, jakie kroki podjął administrator aby zapewnić skuteczność wprowadzonych rozwiązań, a w szczególności, czy i w jaki sposób przeprowadzana była weryfikacja ich przestrzegania przez osoby mające dostęp do danych osobowych, w tym przez kuratorów.
2. Określenia, czy, a jeśli tak, to w jaki sposób zagubiony nośnik został zabezpieczony przed dostępem do danych osobowych przy jego użyciu przetwarzanych.
3. Wskazania, czy zabezpieczenia zostały implementowane przez administratora przed wydaniem nośnika do użytku, czy też kurator był zobowiązanych do ich zastosowania osobiście.
4. Udzielenia informacji, czy przed wystąpieniem przedmiotowego naruszenia, kuratorzy zostali zapoznani z wdrożonymi procedurami i rozwiązaniami.
5. Wskazania, czy przed wystąpieniem przedmiotowego naruszenia ochrony danych osobowych, administrator przeprowadził analizę ryzyka możliwości wystąpienia naruszenia w tym zakresie.
6. Udzielenia informacji, czy, a jeśli tak, to kiedy i w jaki sposób, administrator dokonywał regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, których naruszenie dotyczy.

W odpowiedzi Administrator pismem z dnia [...] października 2020 r. wyjaśnił, iż przed wystąpieniem naruszenia wdrożył system ochrony danych osobowych w postaci zasad przetwarzania danych osobowych, które zostały określone w Polityce Bezpieczeństwa Sądu Rejonowego w Zgierzu i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Sądzie Rejonowym w Zgierzu. System ten funkcjonuje w strukturze administratora od [...] listopada 2017 r., zaś wdrożona dokumentacja jest na bieżąco aktualizowana, audytowana przez powołanego do tego celu inspektora ochrony danych. Zgodnie z załączonym do pisma załącznikiem nr 4 „Zasady ochrony nośników danych po aktualizacji z dnia [...] maja 2018 r.", *„zabrania się korzystania i przetwarzania służbowych danych z wykorzystywaniem prywatnych nośników informacji (w tym pamięci typu flash, płyt cd, pendrive i dysków zewnętrznych)"*. Aby zaś zapewnić skuteczność wdrożonych rozwiązań Sąd podejmował działania w postaci szkoleń stacjonarnych oraz e-lerningowych, prowadzonych dla pracowników Sądu (w tym kuratorów), dotyczące ochrony danych osobowych oraz zapisów wdrożonej dokumentacji, dyżurów pełnionych przez inspektora ochrony danych w siedzibie administratora, dyżurów on-line oraz doraźnych kontroli prowadzonych przez inspektora ochrony danych podczas dyżurów.

Jak dalej wskazał Administrator, zgodnie z treścią Instrukcji Zarządzania Systemem Informatycznym obowiązek zabezpieczenia nośnika spoczywa na użytkowniku, który dokonał jego zabezpieczenia poprzez przechowywanie go w zamykanej torbie służbowej, natomiast po wystąpieniu przedmiotowego naruszenia została zaktualizowana procedura dotycząca wydawania nośników danych, poprzez wprowadzenie ewidencjonowania, szyfrowania i zabezpieczania nośników hasłem. Wszyscy pracownicy Sądu, w tym kuratorzy, przechodzą szkolenia z zakresu ochrony danych i zasad postępowania z danymi przetwarzanymi w Sądzie Rejonowym w Zgierzu. Szkolenia są prowadzone przez platformę e-lerningową, po odbyciu takiego szkolenia pracownik musi zaliczyć test wiedzy, dopiero po zaliczeniu testu system generuje zaświadczenie i upoważnienie do przetwarzania danych osobowych, którego integralną częścią jest oświadczenie o zapoznaniu się z dokumentacją, jak również w formie tradycyjnej, prowadzonej przez inspektora ochrony danych. Administrator przeprowadził również analizę ryzyka możliwości wystąpienia tego typu naruszenia w postaci zagubienia sprzętu lub nośników, definiując ryzyko na poziomie średnim oraz wskazując konieczność ograniczenia tego ryzyka, przyjął za wystarczający środek ograniczający możliwość zmaterializowania się tego ryzyka w postaci szkolenia dla personelu, dotyczącego potencjalnych zagrożeń.

W zakresie zaś regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, w kontekście realizacji obowiązków wynikających m.in. z art. 32 ust. 1 lit. d) rozporządzenia 2016/679, Administrator wskazał, iż inspektor ochrony danych w porozumieniu z Dyrektorem Sądu przeprowadza doraźne sprawdzenia w poszczególnych wydziałach sądu podczas wizyt zgodnych z harmonogramem dyżurów. W przypadkach szczególnych sprawdzenie jest dokonywane na prośbę kierownika wydziału, natomiast testowanie, mierzenie i ocena zabezpieczeń systemowych i ich skuteczności prowadzone jest przez dział IT. Nie przedstawił natomiast dokumentacji potwierdzającej wykonanie jakiegokolwiek testowania, mierzenia i oceniania skuteczności wdrożonych środków technicznych i organizacyjnych.

Administrator wskazał również, iż po wystąpieniu przedmiotowego naruszenia, zgodnie z zarządzeniem nr [...] Prezesa Sądu Rejonowego w Zgierzu z dnia [...] lutego 2020 r., wszystkie pamięci przenośne zostały zabezpieczone aplikacją szyfrującą.

W związku z powyższym, w dniu [...] marca 2021 r. Prezes Urzędu wezwał Sąd do przedstawienia kolejnych wyjaśnień, w postaci wskazania przepisów, stanowiących podstawę prawną wyznaczenia kuratora sądowego w odniesieniu do każdej z przyznanych mu do prowadzenia spraw, w ramach których dane osobowe były przetwarzane na zagubionym nośniku pamięci.

W odpowiedzi przesłanej do organu nadzorczego [...] kwietnia 2021 r. Administrator wskazał, iż obowiązki i uprawnienia kuratorów sądowych oraz prawne uwarunkowania tej funkcji określa ustawa z dnia 21 lipca 2001r. o kuratorach sądowych (Dz. U. z 2020 r., poz. 167), zwana dalej „ustawą o kuratorach sądowych". Po nowelizacji z dnia 21 lutego 2019 r. i dodaniu art. 9a – kuratorzy są w pełni legitymizowani do zbierania i przetwarzania informacji niezbędnych w powierzonych sprawach. Nadzory były zlecane na mocy § 2 rozporządzenia Ministra Sprawiedliwości z dnia 12 czerwca 2003 r. w sprawie szczegółowego sposobu wykonywania uprawnień i obowiązków kuratorów zawodowych (Dz.U. z 2014 r., poz. 795), natomiast wywiady środowiskowe były zlecane do przeprowadzenia kuratorowi w następujących rodzajach spraw:

- w sprawach małżeńskich (art. 434 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2020 r., poz. 1575), zwanej dalej „kpc", w zw. z art. 56 § 2, 58 § l i 61^1 § 2 ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (Dz. U. z 2020 r., poz. 1359);
- w sprawach o rozstrzygnięcie w istotnych sprawach rodziny (art. 565^1 kpc);
- w sprawach opiekuńczych małoletnich (art. 570^1 kpc);
- w sprawach dot. ustanowienia opieki lub kurateli i prowadzonego w sprawach postępowania wykonawczego w celu ustalenia możliwości lub sposobu sprawowania opieki lub kurateli oraz warunków życiowych osoby, której postępowanie dotyczy (art. 570^{1a} kpc);
- w sprawach o przysposobienie dziecka (art. 9 Europejskiej Konwencji o przysposobieniu dzieci); - w postępowaniu wyjaśniającym i rozpoznawczym w sprawach nieletnich (art. 24 ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2018 r., poz. 969);
- w celu ustalenia okoliczności wskazujących na nadużywanie alkoholu przez osobę, której postępowanie dotyczy oraz zakłócania przez nią spokoju lub porządku publicznego, a także jej relacji w rodzinie, zachowania się w stosunku do małoletnich i stosunku do pracy (art. 30a ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałania alkoholizmowi (Dz. U. z 2019 r., poz. 2277);
- w celu ustalenia warunków życiowych osoby, której postępowanie dotyczy oraz jej funkcjonowania w środowisku (art. 42a ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 2020 r., poz. 685);
- wywiady kontrolne przeprowadzane przez zawodowych kuratorów sądowych w nadzorach wykonywanych przez kuratorów społecznych oraz inne uprawnione osoby (art. 11 pkt 4 ustawy o kuratorach sądowych oraz § 5 pkt 2 rozporządzenia Rady Ministrów z dnia 12 czerwca 2003 r. w sprawie szczegółowego sposobu wykonywania uprawnień i obowiązków kuratorów sądowych (Dz. U. z 2014 r., poz. 989).

Dalej Administrator wyjaśnił, iż tryb wykonywania wywiadów przez kuratora rodzinnego został określony w § 6-8 rozporządzenia Ministra Sprawiedliwości w sprawie szczegółowego sposobu wykonywania uprawnień i obowiązków kuratorów sądowych oraz w rozporządzeniu Ministra Sprawiedliwości z dnia 16 sierpnia 2001 r. w sprawie szczegółowych zasad i trybu przeprowadzania wywiadów środowiskowych o nieletnich (Dz. U. z 2001, nr 90, poz. 1010). Ponadto wskazał, iż do przeprowadzania wywiadu przez kuratora rodzinnego stosuje się odpowiednio przepisy § 1 ust. l i 2, § 2, § 3, § 4 i § 7 rozporządzenia Ministra Sprawiedliwości z dnia 11 czerwca 2003 r. w sprawie regulaminu czynności w zakresie przeprowadzania wywiadu środowiskowego oraz wzoru kwestionariusza tego wywiadu (Dz. U. z 2003 r., Nr 108., poz. 1018).

Zgodnie z art. 9b ustawy o kuratorach sądowych, administratorem danych przetwarzanych w celu wykonania zadań lub obowiązków przez kuratora sądowego jest prezes sądu, w którym kurator sądowy pełni obowiązki służbowe.

Jak wynika z dokonanych ustaleń, naruszenie ochrony danych osobowych, zgłoszone Prezesowi Urzędu i zarejestrowane pod sygn. [...], polegało na zgubieniu przez kuratora sądowego nieszyfrowanej przenośnej pamięci typu pendrive, przy użyciu której były przetwarzane dane osobowe 400 osób, podlegających nadzorowi kuratorskiemu i objętych wywiadem środowiskowym przez kuratora, w zakresie imion i nazwisk, dat urodzenia, adresów zamieszkania lub pobytu, numerów ewidencyjnych PESEL, danych dotyczących zarobków i/lub posiadanego majątku, serii i numerów dowodów osobistych, numerów telefonów, danych dotyczących zdrowia oraz danych dotyczących wyroków skazujących. Tym samym, stosownie do przywołanego wyżej przepisu ustawy o kuratorach sądowych, administratorem danych przetwarzanych przez kuratora sądowego na zagubionym nośniku jest Prezes Sądu Rejonowego w Zgierzu, a nie Sąd.

Wobec powyższego, pismem z dnia [...] maja 2021 r. Prezes Urzędu wszczął z urzędu postępowanie administracyjne, wobec naruszenia przez Prezesa Sądu Rejonowego w Zgierzu, jako administratora danych, obowiązków wynikających z rozporządzenia 2016/679, tj. art. 5 ust. 1 lit. f), art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2, w związku z ww. naruszeniem ochrony danych osobowych (sygn. DKN.5131.22.2021). Ponadto, na podstawie art. 123 § 1 oraz art. 75 § 1 k.p.a. w zw. z art. 7 ust. 1 ustawy o ochronie danych osobowych Prezes Urzędu wydał [...] maja 2021 r. postanowienie o sporządzeniu uwierzytelnionych odpisów z akt postępowania o sygnaturze [...], tj.: zawiadomienia o wszczęciu postępowania administracyjnego wobec Sądu Rejonowego w Zgierzu z dnia [...] września 2020 r., odpowiedzi z dnia [...] października 2020 r., wezwania do złożenia dodatkowych wyjaśnień z dnia [...] lutego 2021 r., odpowiedzi z dnia [...] marca 2021 r., wezwania do złożenia wyjaśnień z dnia [...] marca 2021 r. oraz odpowiedzi z dnia [...] kwietnia 2021 r., w celu ich włączenia do postępowania prowadzonego pod sygnaturą DKN.5131.22.2021.

Po rozpatrzeniu całości materiału dowodowego zebranego w sprawie Prezes Urzędu Ochrony Danych Osobowych zważył, co następuje:

Art. 5 rozporządzenia 2016/679 wskazuje zasady dotyczące przetwarzania danych osobowych, które muszą być respektowane przez wszystkich administratorów, tj. podmioty wskazane prawem Unii lub prawem państwa członkowskiego oraz 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 („integralność i poufność").

Zgodnie z treścią 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.

Przepis art. 24 ust. 1 rozporządzenia 2016/679 określa podstawowe i główne obowiązki administratora, którego obciąża wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających zgodność przetwarzania z wymogami rozporządzenia 2016/679. Chodzi tu w szczególności o realizację zasad wskazanych w art. 5 ust. 1 rozporządzenia 2016/679.

Zgodnie natomiast 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 zagrożenia 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 rozporządzenia oraz chronić prawa osób, których dane dotyczą (uwzględnianie ochrony danych w fazie projektowania).

Stosownie do art. 32 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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (lit. b) oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (lit. d).

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.

Przepisy art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679, wraz z art. 24 ust. 1 ww. rozporządzenia, stanowią więc konkretyzację wskazanej w art. 5 ust. 1 lit. f) rozporządzenia 2016/679, zasady integralności i poufności.

Poufność danych to właściwość zapewniająca w szczególności, że dane nie zostaną udostępnione nieuprawnionym podmiotom, uzyskiwana między innymi dzięki zastosowaniu środków technicznych i organizacyjnych, adekwatnych do zakresu danych, kontekstu przetwarzania oraz zidentyfikowanych ryzyk. Wskazana zasada, jak wynika z ustalonego stanu faktycznego, została naruszona przez Prezesa Sądu poprzez wydanie do użytku służbowego kuratorom sądowym niezabezpieczonego przenośnego nośnika pamięci oraz zobowiązanie ich do wdrożenia zabezpieczeń tej pamięci we własnym zakresie, co w następstwie zagubienia takiego nośnika przez kuratora sądowego skutkowało umożliwieniem osobom nieuprawnionym dostępu do danych osobowych przetwarzanych na tym nośniku. Jak bowiem ustalono, jedynym zabezpieczeniem zastosowanym przez kuratora było przechowywanie nośnika w zamykanej torbie służbowej.

Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 3 września 2020 r. o sygnaturze II SA/Wa 2559/19, *„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. 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.”

W kontekście przywołanego wyroku wskazać należy, że analiza ryzyka przeprowadzana przez administratora danych osobowych 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.

Ponadto, aby zrealizować wymóg art. 32 ust. 1 lit. d) rozporządzenia 2016/679, wskazany zresztą w ww. wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie jako obowiązek zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wdrożonych zabezpieczeń, administrator danych osobowych winien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania.

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, ma charakter ciągłego procesu. Winna więc następować okresowa weryfikacja zarówno adekwatności, jak i skuteczności zastosowanych zabezpieczeń.

Przedstawiona w toku postępowania administracyjnego przez Administratora analiza ryzyka przeprowadzona przed wystąpieniem przedmiotowego naruszenia, przedstawia wynik na poziomie 6 dla zagrożenia „Zagubienie sprzętu, nośników". Zgodnie z przedstawioną dokumentacją jest to średni poziom ryzyka, skutkujący koniecznością wdrożenia zabezpieczeń, celem jego obniżenia do poziomu niskiego (uznawanego za akceptowalny poziom), zaś jako reakcję na ryzyko przyjęto i zastosowano działania ograniczające to ryzyko wyłącznie w postaci „Szkolenia dla personelu dotyczącego potencjalnych zagrożeń". Oczywiście szkolenie o tego typu tematyce jest konieczne i potrzebne, albowiem spowodować może chociażby zwiększenie świadomości personelu. Niemniej w odniesieniu do zakresu oraz charakteru danych osobowych przetwarzanych w tym przypadku przy użyciu tego typu urządzenia szkolenie nie jest środkiem organizacyjnym, który pozwoli na obniżenie do niskiego poziomu lub wyeliminowanie ryzyka zagubienia nośnika. Nie zastąpi również rozwiązań o charakterze technicznym, których nie przewidziano. Zgodnie natomiast z tabelą przedstawiającą wynik szacowania ryzyka oraz reakcję na ryzyko, w zależności od jego wysokości, dla „Reakcji na ryzyko" określonej jako „O – ograniczanie", administrator danych przewiduje „Szkolenia, dodatkowe zabezpieczenia techniczne lub organizacyjne", lecz w tym przypadku sam ogranicza się wyłącznie do szkolenia, natomiast faktyczne zabezpieczanie nośnika pozostawia jego użytkownikowi, nie wskazując żadnych przykładowych, określonych przez Prezesa Sądu jako adekwatnych zabezpieczeń, które pracownik może zastosować. Działania tego typu nie mogą zatem zostać uznane jako wdrożenie odpowiednich środków technicznych czy organizacyjnych w kontekście art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 rozporządzenia 2016/679 (w szczególności w celu zapewnienia zdolności do ciągłego zapewnienia poufności danych), albowiem pracownik przede wszystkim nie może zastępować administratora danych w realizacji jego zadań wynikających z tych przepisów. Ponadto, pracownik może nie posiadać w tym zakresie odpowiedniej wiedzy, zignorować konieczność zabezpieczenia nośnika (tak jak miało to miejsce w niniejszym przypadku – kurator sądowy zabezpieczył nośnik wyłącznie poprzez jego przechowywanie w zamykanej torbie, co nie stanowi zabezpieczenia samego nośnika) lub wdrożyć zabezpieczenie nieadekwatne do zakresu i charakteru danych oraz ryzyk występujących w tym procesie przetwarzania danych. Podkreślić należy, że tak zorganizowany proces określania i wdrażania zabezpieczeń przetwarzanych danych osobowych skutkuje wręcz pozbawieniem administratora danych podstawowych informacji niezbędnych do przeprowadzenia w sposób właściwy analizy ryzyka i na tej podstawie zbudowania skutecznego systemu ochrony danych, niezbędnego do ciągłego zapewniania poufności danych, zgodnie z wymogiem wynikającym w szczególności z art. 32 ust. 1 lit. b) rozporządzenia 2016/679, albowiem nie będzie on miał wiedzy co do tego, jakie zabezpieczenia w jego organizacji istnieją, na ile i w przypadku jakich zagrożeń będą skuteczne, a także zostaje pozbawiony informacji oraz możliwości zareagowania na wdrożenie zabezpieczenia nieadekwatnego do zagrożeń. Ponadto należy mieć na uwadze również możliwość wystąpienia nowego, nieznanego dotąd ryzyka lub zagrożenia, mogącego zmaterializować się lub zaistnieć przy wdrożeniu nowego zabezpieczenia, w szczególności jeśli takie wdrożenie odbyło się w sposób nieprawidłowy.

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.

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.

Przedstawione w toku postępowania administracyjnego „Wytyczne do oceny prawdopodobieństwa wystąpienia i następstw ryzyka" w kolumnie „Następstwa (wpływ) dla osoby fizycznej, której dane dotyczą" dla każdego oszacowanego ryzyka od 1 (znikome) przez 2 (niskie), 3 (średnie), 4 (wysokie) do 5 (bardzo wysokie) wskazują tożsame następstwa dla osoby fizycznej w postaci: „utrata reputacji, kara finansowa, utrata klienta, niemożność świadczenia usług, konsekwencje prawne". Natomiast w motywach 75 i 85 preambuły rozporządzenia 2016/679, wśród możliwych negatywnych konsekwencji dla osoby fizycznej, wskazano powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych takich jak: utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

Stwierdzić więc należy, iż przedstawiona analiza ryzyka nie została przeprowadzona właściwie z powodu wskazania nieadekwatnych dla osób fizycznych następstw naruszenia ochrony danych osobowych oraz przyjęcia niewłaściwych środków bezpieczeństwa – wyłącznie organizacyjnych – z całkowitym pominięciem środków technicznych, np. w postaci szyfrowania pamięci przenośnych, mających na celu obniżenie ryzyka do poziomu akceptowalnego. Ponadto stwierdzić należy, iż rozwiązanie przyjęte w tym zakresie przez administratora danych (tylko szkolenia pracowników) podważa skuteczność wdrożonego systemu ochrony danych osobowych, albowiem jak wskazano powyżej, efektem przeprowadzonej analizy ryzyka winien być odpowiedni dobór środków zarówno technicznych, jak i organizacyjnych, a więc konkretnych środków, które zminimalizują zidentyfikowane ryzyka. Natomiast pozostawienie doboru i wdrożenia środków zabezpieczających osobie, która otrzymała do użytku niezabezpieczoną pamięć przenośną, oznacza, iż Prezes Sądu pozbawił siebie jako administratora danych podstawowych i kluczowych informacji, niezbędnych w kontekście realizacji obowiązków wynikających z art. 32 ust. 2 rozporządzenia 2016/679.

W tym kontekście należy wskazać, że Wojewódzki Sąd Administracyjny w Warszawie w wyroku o sygnaturze II SA/Wa 2826/19 z dnia 26 sierpnia 2020 r. 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."*

Podkreślenia wymaga, że Prezes Sądu dla prawidłowej realizacji obowiązków wynikających z wyżej przywołanych przepisów rozporządzenia 2016/679 nie powinien w ogóle stosować niezabezpieczonych przenośnych nośników pamięci. Dopuszczając zaś możliwość przetwarzania danych osobowych przy ich użyciu, w oparciu o właściwie przeprowadzoną analizę ryzyka, winien

określić oraz wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych osobowych, a następnie regularnie sprawdzać skuteczność działania tych środków. Wskazać ponownie należy, że stosownie do art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 to administrator danych, nie zaś pracownik lub osoba wykonująca zadania służbowe, jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z wymaganiami wskazanego rozporządzenia. Do przedmiotowego naruszenia ochrony danych osobowych osób fizycznych doszło w wyniku niezastosowania zabezpieczenia przenośnego nośnika pamięci, co dało możliwość dostępu do danych osobowych przy jego użyciu przetwarzanych osobom nieuprawnionym.

Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku o sygnaturze II SA/Wa 2826/19 z dnia 26 sierpnia 2020 r. *„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. (...) 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”.*

W przyjętych przez Prezesa Sądu zarządzeniem nr [...] Prezesa i Dyrektora Sądu Rejonowego w Zgierzu z dnia [...] listopada 2017 r. Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Sądzie Rejonowym w Zgierzu nie wskazano uregulowań zapewniających regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych, co również przyczyniło się do wystąpienia naruszenia ochrony danych osobowych.

Pomimo wezwania do przedstawienia dokumentacji potwierdzającej działania podjęte przez administratora, celem zapewnienia skuteczności wprowadzonych rozwiązań oraz potwierdzenia przeprowadzanego regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, Prezes Sądu w piśmie z [...] października 2020 r. ograniczył się jedynie do stwierdzenia, iż inspektor ochrony danych przeprowadza doraźne sprawdzenia w poszczególnych wydziałach sądu zgodnie z harmonogramem dyżurów, zaś testowanie, mierzenie i ocena zabezpieczeń systemowych i ich skuteczności prowadzone jest przez dział IT nie przedstawiając, pomimo wezwania, jakiejkolwiek dokumentacji potwierdzającej, iż kiedykolwiek tego typu działania zostały podjęte.

Ponadto zaznaczyć należy, iż prowadzenie „doraźnych sprawdzeń” nie wyczerpuje znamion regularności. W ocenie Prezesa Urzędu dokonywanie sprawdzeń doraźnie, bez przyjęcia procedury, która określa harmonogram działań zapewniających regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków jest niewystarczające. Ponadto, działania doraźne stanowią

zwykle reakcję na pojawiające się zagrożenia, materializujące się ryzyka wystąpienia zdarzeń lub sytuacji niepożądanych bądź reakcję na zgłaszane lub ujawniane luki w stosowanym systemie ochrony danych osobowych. Nie są natomiast efektem zaplanowanych działań mających na celu weryfikację skuteczności wdrożonych zabezpieczeń. W żadnym wypadku nie można przypisać im również atrybutu regularności.

Podkreślenia wymaga, że regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania jest podstawowym obowiązkiem każdego administratora oraz podmiotu przetwarzającego wynikającym nie tylko z art. 32 ust. 1 lit. d) rozporządzenia 2016/679, ale również z faktu, iż podczas realizacji poszczególnych czynności przetwarzania mogą pojawić się lub zaistnieć nowe ryzyka dla bezpieczeństwa tego przetwarzania nieznane lub niezidentyfikowane wcześniej. Administrator zobowiązany jest więc do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania. Kompleksowość tej weryfikacji powinna być oceniana przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania. Natomiast w przedmiotowym stanie faktycznym Prezes Sądu nie wywiązywał się z tego obowiązku.

Testowanie, mierzenie i ocenianie skuteczności przyjętych środków bezpieczeństwa, aby stanowiło realizację wymogu wynikającego z art. 32 ust. 1 lit. d) rozporządzenia 2016/679, musi być dokonywane w sposób regularny, co oznacza świadome zaplanowanie i zorganizowanie, a także dokumentowanie (w związku z zasadą rozliczalności, o której mowa w art. 5 ust. 2 rozporządzenia 2016/679) tego typu działań w określonych przedziałach czasowych, niezależnie od np. zmian w organizacji i przebiegu procesów przetwarzania danych. Takich działań Prezes Sądu jednak nie podejmował. Podkreślić również należy, że pozostawienie wyboru sposobu zabezpieczenia przenośnego nośnika pamięci wykorzystywanej do przetwarzania danych osobowych oraz jego wdrożenia osobie będącej jej użytkownikiem pozbawia administratora wiedzy o istotnych elementach systemu ochrony danych osobowych, co z kolei uniemożliwia prawidłową realizację obowiązku wskazanego w art. 32 ust. 1 lit. d) rozporządzenia 2016/679.

Zatem brak rzetelnie przeprowadzonej analizy ryzyka, w połączeniu z brakiem regularnego testowania, mierzenia i oceniania skuteczności wdrożonych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania oraz niewprowadzeniem środków technicznych i organizacyjnych zabezpieczających dane osobowe przetwarzane przy użyciu przenośnych nośników pamięci, doprowadził, co należy ponownie podkreślić, do naruszenia danych ochrony danych, ale też przesądza o naruszeniu przez Prezesa Sądu obowiązków spoczywających na administratorze danych, wynikających z art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b) i lit. d) oraz art. 32 ust. 2 rozporządzenia 2016/679, a w konsekwencji również zasady wyrażonej w art. 5 ust. 1 lit. f) rozporządzenia 2016/679.

Podkreślenia również wymaga, że powołany art. 25 ust. 1 rozporządzenia 2016/679 pomimo nazwania wskazanego w nim obowiązku administratora jako „ochrona danych w fazie projektowania” dotyczy nie tylko etapu projektowania, ale także samego etapu przetwarzania danych. Wdrażanie zabezpieczeń stanowi bowiem ciągły proces, a nie tylko jednorazowe działanie administratora. Wymienione w nim środki, jak „minimalizacja danych” czy też „pseudonimizacja”,

są tylko przykładem środków, które powinny zostać zastosowane w celu spełnienia wymogu realizacji zasad ochrony danych oraz nadania przetwarzaniu niezbędnych zabezpieczeń, by spełnić wymogi rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Wskazać zatem ponownie należy, że obowiązkiem każdego administratora jest przetwarzanie danych zgodnie z zasadami określonymi art. 5 rozporządzenia 2016/679, w tym przypadku zgodnie z art. 5 ust. 1 lit. f).

Podsumowując, pomimo usunięcia przez Prezesa Sądu uchybień w zakresie bezpieczeństwa danych przetwarzanych przy użyciu przenośnych nośników pamięci, w tym poprzez zastosowanie szyfrowania tych nośników, którego brak był przyczyną naruszenia poufności danych osobowych, zaistniały przesłanki uzasadniające zastosowanie wobec Prezesa Sądu przysługujących Prezesowi Urzędu uprawnień do nałożenia kary administracyjnej za naruszenie zasady poufności danych (art. 5 ust. 1 lit. f) rozporządzenia 2016/679), w związku z naruszeniem obowiązków administratora przy wdrażaniu środków technicznych i organizacyjnych w trakcie przetwarzania danych, w celu skutecznej realizacji zasad ochrony danych (art. 25 ust. 1 rozporządzenia 2016/679), obowiązków w zakresie zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych (art. 32 ust. 1 lit. b) rozporządzenia 2016/679), obowiązku regularnego testowania, mierzenia i oceniania skuteczności przyjętych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1 lit. d) rozporządzenia 2016/679) oraz obowiązku uwzględnienia ryzyka wiążącego się z przetwarzaniem, wynikającego z nieuprawnionego dostępu do przetwarzanych danych osobowych (art. 32 ust. 2 rozporządzenia 2016/679).

Skorzystanie przez Prezesa Urzędu z przysługującego mu uprawnienia wynika przede wszystkim z faktu, iż administrator uchybił jednej z podstawowych zasad przetwarzania danych, tj. zasadzie poufności, wyrażonej w art. 5 ust. 1 lit. f) 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.

Decydując o nałożeniu na Prezesa Sądu administracyjnej kary pieniężnej, a także określając jej wysokość, Prezes Urzędu Ochrony Danych Osobowych – stosownie do treści art. 83 ust. 2 lit. a) – k) rozporządzenia 2016/679 – wziął pod uwagę, i uznał za obciążające dla Prezesa Sądu, następujące okoliczności sprawy:

a) Charakter i waga naruszenia, liczba poszkodowanych osób (art. 83 ust. 2 lit. a rozporządzenia 2016/679).

Stwierdzone w niniejszej sprawie naruszenie, którego skutkiem była możliwość uzyskania nieuprawnionego dostępu do przetwarzanych przez Prezesa Sądu danych przez osobę bądź osoby nieuprawnione, a w konsekwencji pozyskanie danych osobowych osób, wobec których były podejmowane działania przez kuratora sądowego, ma znaczną wagę i poważny charakter, stwarza bowiem wysokie ryzyko negatywnych skutków prawnych dla dużej liczby osób, do których danych dostęp mogła mieć osoba bądź osoby nieuprawnione. Naruszenie przez Prezesa Sądu obowiązków

zastosowania środków zabezpieczających przetwarzane dane przed ich udostępnieniem osobom nieuprawnionym, 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, przede wszystkim ze względu na szeroki zakres danych osobowych, tj.: imiona i nazwiska, daty urodzenia, adresy zamieszkania lub pobytu, numery ewidencyjne PESEL, dane dotyczące zarobków i/lub posiadanego majątku, serie i numery dowodów osobistych, numery telefonów, dane dotyczące zdrowia oraz dane dotyczących wyroków skazujących, dotyczące czterystu (400) osób fizycznych pozostających pod nadzorem kuratora.

b) Czas trwania naruszenia (art. 83 ust. 2 lit. a rozporządzenia 2016/679).

Za okoliczność obciążającą Prezes Urzędu uznaje długi czas trwania naruszenia, ponieważ wprowadzenie ewidencjonowania przenośnych nośników danych oraz szyfrowanie danych przetwarzanych przy ich użyciu nastąpiło dopiero w związku z wydaniem przez Prezesa Sądu Rejonowego w Zgierzu zarządzenia nr [...] z dnia [...] lutego 2020 r. Podkreślić jednocześnie jednak należy, że konsekwencje naruszenia przepisów rozporządzenia 2016/679 przez administratora danych trwają nadal, ponieważ zaginiony niezabezpieczony nośnik pamięci nie został do tej pory odnaleziony, więc w dalszym ciągu osoba lub osoby nieuprawnione mogą mieć dostęp do danych osobowych znajdujących się na tym nośniku, czego konsekwencją jest wysokie ryzyko naruszenia praw lub wolności tych osób.

c) Rozmiar szkody poniesionej przez osoby, których dotyczyło naruszenie (art. 83 ust. 2 lit. a 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.

d) Nieumyślny charakter naruszenia (art. 83 ust. 2 lit. b rozporządzenia 2016/679).

Nieuprawniony dostęp do danych osobowych osób, wobec których były podejmowane działania przez kuratora, stał się możliwy na skutek niedochowania należytej staranności przez Prezesa Sądu i niewątpliwie stanowi o nieumyślnym charakterze naruszenia. Niemniej jednak Prezes Sądu jako administrator ponosi odpowiedzialność za stwierdzone nieprawidłowości w procesie przetwarzania danych. Na negatywną ocenę zasługuje fakt, że Prezes Sądu przeniósł obowiązek zabezpieczenia nośnika na kuratora sądowego, nie zweryfikował, czy kurator sądowy w jakikolwiek sposób dokonał jego zabezpieczenia oraz nie przeprowadził testu pod kątem skuteczności tego zabezpieczenia. W tym stanie rzeczy, zaniedbanie Prezesa Sądu należy uznać za rażące.

e) Stopień odpowiedzialności Prezesa Sądu z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez niego na mocy art. 25 i 32 rozporządzenia 2016/679 (art. 83 ust. 2 lit. d rozporządzenia 2016/679).

Zgodnie z przywołanymi przepisami to na administratorze danych osobowych ciąży obowiązek przede wszystkim określenia, jakie środki techniczne i organizacyjne będą odpowiednie w odniesieniu do zidentyfikowanych ryzyk naruszenia praw lub wolności osób fizycznych,

wdrożenia odpowiednich środków technicznych i organizacyjnych oraz obowiązek ich oceniania na każdym etapie przetwarzania. W przedmiotowej sprawie administrator nie podjął jednak działań mających na celu realizację obowiązków wynikających z ww. przepisów rozporządzenia 2016/679, tj. nie wdrożył adekwatnych do poziomu ryzyka środków technicznych i organizacyjnych zapewniających poufność przetwarzanych danych, a co więcej przerzucił ten obowiązek na kuratorów sądowych. Przeniesienie obowiązków administratora danych osobowych w zakresie wyboru oraz zastosowania odpowiednich środków technicznych na inne osoby skutkowało bowiem w tym przypadku zastosowaniem środka technicznego w postaci przechowywania przenośnego nośnika pamięci w zamykanej torbie służbowej, a więc zupełnie nieadekwatnego w odniesieniu do stanu wiedzy technicznej, kosztu wdrożenia oraz charakteru, zakresu, kontekstu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwa wystąpienia i wadze zagrożenia.

f) Kategorie danych osobowych, których dotyczyło naruszenie (art. 83 ust. 2 lit. g).

Naruszenie ochrony danych osobowych w postaci imion i nazwisk, dat urodzenia, adresów zamieszkania lub pobytu, numerów ewidencyjnych PESEL, danych dotyczących zarobków i/lub posiadanego majątku, serii i numerów dowodów osobistych, numerów telefonów oraz danych podlegających szczególnej ochronie zgodnie z art. 9 rozporządzenia 2016/679 (danych dotyczących zdrowia), a także danych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 rozporządzenia 2016/679, skutkować może szerokim wachlarzem negatywnych skutków dla osób, których dane dotyczą. Jak wskazuje się w motywie 75 preambuły rozporządzenia 2016/679, *„Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa (...)”*. Z kolei z motywu 85 preambuły rozporządzenia 2016/679 wynika, że *„Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze społeczne (...)”*. Ponadto zauważyć należy, iż przetwarzanie danych osobowych szczególnych kategorii, określonych w art. 9 rozporządzenia 2016/679 oraz

danych dotyczących wyroków skazujących, wskazanych w art. 10 rozporządzenia 2016/679, z racji swego zakresu, a co za tym idzie możliwych negatywnych konsekwencji ich ujawnienia, skutkować winno wprowadzeniem zdecydowanie wyższego poziomu ochrony tych danych osobowych.

Ustalając wysokość administracyjnej kary pieniężnej, Prezes Urzędu Ochrony Danych Osobowych uwzględnił jako okoliczność łagodzącą, mającą wpływ na obniżenie wysokości wymierzonej kary, **dobrą współpracą Prezesa Sądu z organem nadzorczym podjętą i prowadzoną 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 Prezes Sądu prawidłowo wywiązał się z ciążących na nim obowiązków procesowych w trakcie postępowania administracyjnego, zakończonego wydaniem niniejszej decyzji. Prezes Sądu podjął również konkretne i szybkie działania, których efektem było usunięcie możliwości wystąpienia naruszenia. W szczególności Prezes Sądu usunął podatność na naruszenie ochrony przetwarzanych danych osobowych, w terminie 8 dni od wystąpienia naruszenia wydał zarządzenie określające nowe zasady postępowania z pamięciami przenośnymi, następnie w terminie kolejnych 14 dni wprowadził ewidencjonowanie i szyfrowanie użytkowanych przenośnych pamięci oraz powiadomił osoby fizyczne o wystąpieniu naruszenia ochrony ich danych osobowych poprzez zamieszczenie komunikatu o stwierdzonym naruszeniu ochrony danych osobowych.

Na fakt zastosowania przez Prezesa Urzędu w niniejszej sprawie sankcji w postaci administracyjnej kary pieniężnej, jak również na jej wysokość, nie miały inne, wskazane w art. 83 ust. 2 rozporządzenia 2016/679, okoliczności:
a) działania podjęte przez Prezesa Sądu w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą (art. 83 ust. 2 lit. c rozporządzenia 2016/679) – działania takie nie zostały podjęte;
b) stosowne wcześniejsze naruszenia przepisów rozporządzenia 2016/679 dokonane przez Prezesa Sądu (art. 83 ust. 2 lit. e rozporządzenia 2016/679) – nie stwierdzono innych naruszeń ochrony danych osobowych;
c) sposób w jaki organ nadzorczy dowiedział się o naruszeniu (art. 83 ust. 2 lit h rozporządzenia 2016/679). Zgodnie bowiem z art. 33 ust. 1 rozporządzenia 2016/679 w przypadku naruszenia ochrony danych osobowych, to administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Faktem jest, iż w zgłoszeniu naruszenia ochrony danych osobowych stanowiącego podstawę do wszczęcia postępowania administracyjnego jako administrator danych osobowych wskazany został Sąd Rejonowy w Zgierzu, niemniej faktem również jest, iż w imieniu Sądu działał Prezes Sądu – można zatem przyjąć, że to właśnie ten administrator danych przesłał zgłoszenie naruszenia ochrony danych osobowych, więc należy uznać iż zrealizował obowiązek wskazany w przywołanym powyżej przepisie;
d) 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) – nie były nakładane środki wskazane w art. 58 ust. 2 rozporządzenia 2016/679;
e) 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) – nie były stosowane zatwierdzone kodeksy postępowania;

f) osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty (art. 83 ust. 2 lit. k) – nie stwierdzono osiągnięcia korzyści majątkowych lub uniknięcia strat.

Uwzględniając wszystkie omówione wyżej okoliczności, Prezes Urzędu Ochrony Danych Osobowych uznał, iż nałożenie administracyjnej kary pieniężnej na Prezesa Sądu jest konieczne i uzasadnione wagą, charakterem oraz zakresem zarzucanych Prezesowi Sądu naruszeń. Stwierdzić należy, iż zastosowanie wobec Prezesa Sądu 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), nie byłoby proporcjonalne do stwierdzonych nieprawidłowości w procesie przetwarzania danych osobowych oraz nie gwarantowałoby tego, że Prezes Sądu w przyszłości nie dopuści się kolejnych zaniedbań.

Odnosząc się do wysokości wymierzonej Prezesowi Sądu administracyjnej kary pieniężnej, Prezes Urzędu Ochrony Danych Osobowych uznał, iż w ustalonych okolicznościach niniejszej sprawy – tj. wobec stwierdzenia naruszenia kilku przepisów rozporządzenia 2016/679 (zasady poufności danych, wyrażonej w art. 5 ust. 1 lit. f), a odzwierciedlonej w postaci obowiązków określonych w art. 25 ust. 1, art. 32 ust. 1 lit. b) i lit. d) oraz art. 32 ust. 2) oraz faktu, iż Prezes Sądu jest organem jednostki sektora finansów publicznych – zastosowanie znajdzie również 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 przedstawionym stanie faktycznym za najpoważniejsze należy uznać naruszenie przez Prezesa Sądu zasady poufności określonej w art. 5 ust. 1 lit. f) rozporządzenia 2016/679. Przemawia za tym poważny charakter naruszenia, zakres danych osobowych podlegających naruszeniu oraz krąg osób nim dotkniętych (400 – czterystu osób, których administratorem jest Prezes Sądu). Co istotne, w stosunku do ww. liczby osób w dalszym ciągu istnieje wysokie ryzyko niezgodnego z prawem posłużenia się ich danymi osobowymi, albowiem nieznany jest cel, dla którego osoba bądź osoby nieuprawnione mogą podjąć działania zmierzające do wykorzystania tych danych.

W ocenie Prezesa Urzędu, 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 indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca.

Zdaniem Prezesa Urzędu nałożona na Prezesa Sądu kara będzie skuteczna, albowiem doprowadzi do stanu, w którym Prezes Sądu 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 Prezes Sądu od momentu zakończenia niniejszego postępowania będzie z najwyższą 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 bardzo wysokiego ryzyka negatywnych konsekwencji, jakie w związku z naruszeniem ponoszą. Zdaniem

Prezesa Urzędu, nałożona na Prezesa Sądu 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 Urzędu, Prezes Sądu powinien i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, stąd nałożenie kary w wysokości 10 000 zł (dziesięć tysięcy zł) jest w pełni uzasadnione.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych, administracyjna kara pieniężna spełni w tych konkretnych okolicznościach funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Prezesa Sądu przepisów rozporządzenia 2016/679, ale i prewencyjną, bowiem przyczyni się do zapobiegania w przyszłości naruszania obowiązków Prezesa Sądu wynikających z przepisów o ochronie danych osobowych, zarówno przy przetwarzaniu danych przez samego Prezesa Sądu, jak i w stosunku do podmiotów działających na jego zlecenie.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych, 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 Prezesa Sądu w przyszłości przepisów rozporządzenia 2016/679.

Mając powyższe na uwadze Prezes Urzędu Ochrony Danych Osobowych rozstrzygnął jak w sentencji niniejszej decyzji.