PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH

Warszawa, dnia 17 grudnia 2020 r.

DECYZJA

DKN.5130.1354.2020

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2020 r. poz. 256 ze zm.), art. 7 ust. 1, art. 60, art. 101 i art. 103 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781) oraz art. 57 ust. 1 lit. a, art. 58 ust. 2 lit. i, art. 83 ust. 1-3, art. 83 ust. 4 lit. a oraz art. 83 ust. 5 lit. a w związku z art. 5 ust. 1 lit. f, art. 24 ust. 1, art. 25 ust. 1, art. art. 28 ust. 1, art. 28 ust. 3 lit. h, 32 ust. 1 lit. b i lit. d, art. 32 ust. 2, art. 33 ust. 1, art. 34 ust. 1 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, ze zm.), po przeprowadzeniu postępowania administracyjnego w przedmiocie naruszenia przepisów o ochronie danych osobowych przez ID Finance Poland Sp. z o.o. w likwidacji z siedzibą w Warszawie przy ul. Hrubieszowskiej 6A, Prezes Urzędu Ochrony Danych Osobowych

1) stwierdzając naruszenie przez ID Finance Poland Sp. z o.o. w likwidacji z siedzibą w Warszawie przy ul. Hrubieszowskiej 6A przepisów art. 5 ust. 1 lit. f, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. 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, ze zm.), zwanego dalej „rozporządzeniem 2016/679", polegające na niewdrożeniu przez ID Finance Poland Sp. z o.o. w likwidacji z siedzibą w Warszawie, zarówno w fazie projektowania procesu przetwarzania jak i w czasie samego przetwarzania, odpowiednich środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemu przetwarzania danych osobowych, a także zapewniających zdolność skutecznego i szybkiego stwierdzenia naruszenia ochrony danych osobowych oraz zapewniających regularną ocenę skuteczności tych środków, co skutkowało uzyskaniem przez osoby trzecie nieuprawnionego dostępu do przetwarzanych danych osobowych, nakłada na ID Finance Poland Sp. z o.o. w likwidacji, administracyjną karę pieniężną w wysokości 1.069.850,00 PLN (jeden milion sześćdziesiąt dziewięć tysięcy osiemset pięćdziesiąt złotych);

2) w pozostałym zakresie postępowanie umarza.

UZASADNIENIE

ID Finance Poland Sp. z o.o. w likwidacji (zwana dalej także: „Spółką" lub „administratorem") […] marca 2020 r. i uzupełniająco […] marca 2020 r. dokonała zgłoszenia Prezesowi Urzędu Ochrony Danych Osobowych (zwanemu dalej także „Prezesem UODO") naruszenia ochrony danych osobowych klientów Spółki, które zostało zarejestrowane pod sygnaturą DKN.5130.1354.2020.

Przedmiotem działalności Spółki jest udzielanie pożyczek finansowych z wykorzystaniem serwisu internetowego moneyman.pl. W zgłoszeniu Spółka wskazała, że naruszenie miało miejsce […] marca 2020 r. i zostało stwierdzone […] marca 2020 r. w wyniku potwierdzenia informacji dotyczących możliwości nieautoryzowanego dostępu do danych, otrzymanej od osoby trzeciej. Naruszenie dotyczyło problemów związanych z działaniem serwera, na którym przetwarzane były dane osobowe 218 657 osób. W zgłoszeniu uzupełniającym z […] marca 2020 r. oraz w piśmie z […] marca 2020 r. Spółka doprecyzowała, że dane obejmowały 140 699 klientów Spółki (pierwotna liczba była związana m.in. z liczbą rekordów w bazie danych, a nie liczbą osób fizycznych, których te dane dotyczą), którzy po […] stycznia 2018 r. w całości lub w części przeszli przez proces rejestracji w serwisie moneyman.pl, i dane te obejmowały: imię i nazwisko, poziom wykształcenia, adres e-mail, dane dotyczące zatrudnienia, adres e-mail osoby, której klient chce polecić pożyczkę, dane dotyczące zarobków, dane dotyczące stanu cywilnego, numer telefonu (stacjonarnego, komórkowego, wcześniej używanego numeru telefonu), numer PESEL, narodowość, numer NIP, hasło, miejsce urodzenia, adres korespondencyjny, adres zameldowania, numer telefonu do miejsca pracy oraz numer rachunku bankowego. Błędne działanie serwera związane było z jego restartem przez podmiot przetwarzający – IDFT z siedzibą w M. na B., któremu na podstawie umowy z dnia […] marca 2018 r. powierzono przetwarzanie ww. danych w celu realizacji usług mających charakter hostingu. W trakcie restartu serwera doszło do zresetowania ustawień oprogramowania odpowiadającego za bezpieczeństwo serwera, w konsekwencji czego dane osobowe znajdujące się na serwerze były publicznie dostępne. Baza danych znajdująca się na tym serwerze została pobrana i usunięta przez nieustalony podmiot trzeci, który wystąpił do Spółki z żądaniem zapłaty wynagrodzenia w zamian za jej zwrot. W zgłoszeniu wskazano, że w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą, poinformowano klientów i potencjalnych klientów o zresetowaniu haseł do logowania. W celu zminimalizowania ryzyka ponownego wystąpienia naruszenia m.in. przywrócono prawidłowe działanie zapory firewall. Jednocześnie wskazano, że w ocenie Spółki zachodzi wysokie ryzyko naruszenia praw lub wolności osób fizycznych, których dane dotyczą. W zgłoszeniu uzupełniającym Spółka przekazała, że osoby te zostały zawiadomione o naruszeniu […] marca 2020 r. za pomocą poczty elektronicznej oraz wiadomości sms (treść zawiadomienia stanowiła załącznik do uzupełniającego zgłoszenia).

W związku z powyższym pismem z […] marca 2020 r. Prezes Urzędu Ochrony Danych Osobowych wezwał ID Finance Poland Sp. z o.o. m.in. do:

- przekazania treści umowy powierzenia z podmiotem przetwarzającym biorącym udział w przetwarzaniu, którego naruszenie dotyczy,
- przekazania treści i daty wszelkiej korespondencji kierowanej do Spółki od podmiotów trzecich posiadających wiedzę o przedmiotowym naruszeniu,
- szczegółowego opisu naruszenia ochrony danych osobowych, opisu jego stwierdzenia oraz przedstawienia procedury stwierdzania i zgłaszania naruszeń ochrony danych, również w kontekście relacji z podmiotem przetwarzającym,
- wskazania czasu, kanału i treści innych korespondencji kierowanych w związku z naruszeniem do osób, których dane dotyczą,
- przedstawienia oceny skuteczności dotarcia zawiadomienia o naruszeniu do osób, których dane dotyczą, drogą e-mailową oraz w jaki sposób Spółka zapewnia osobom, których dane dotyczą, skuteczne przekazanie dodatkowych informacji o naruszeniu w ramach funkcjonowania infolinii oraz adresu e-mail, o których mowa w zawiadomieniu skierowanym do tych osób,
- wskazania, czy i jakie Spółka oraz podmiot przetwarzający przyjęły środki zabezpieczenia technicznego i organizacyjnego zgodnie z art. 24 i art. 25 rozporządzenia 2016/679,
- wyjaśnienia, czy, kiedy i w jaki sposób administrator oraz podmiot przetwarzający dokonywali regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

W odpowiedzi, pismem z […] marca 2020 r. Spółka przedstawiła obszerne wyjaśnienia dotyczące samego zdarzenia, w tym kopię korespondencji prowadzonej przez Spółkę. Do wyjaśnień dołączyła również pełną treść umowy powierzenia wraz z załącznikami, zawartej w Warszawie […] marca 2018 r. pomiędzy ID Finance Poland sp. z o.o. z siedzibą w Warszawie a spółką z ograniczoną odpowiedzialnością „IDFT" z siedzibą w M. na B. (dalej zwanej również jako „podmiot przetwarzający"). Wśród przekazanych dokumentów znalazły się również m.in.: Procedura zgłaszania naruszenia ochrony danych osobowych wprowadzona zarządzeniem nr […] z dnia […] maja 2018 r. Zarządu Spółki; Instrukcja w sprawie szczegółowych zasad bezpieczeństwa i zarządzania systemem informatycznym […]; szereg wewnętrznych

procedur i dokumentów stosowanych przez Spółkę oraz podmiot przetwarzający jako element systemu bezpieczeństwa i ochrony danych osobowych. Ponadto, w swoich wyjaśnieniach szczegółowo opisała zastosowane środki techniczne i organizacyjne zarówno przez Spółkę, jak i podmiot przetwarzający.

Jak wynika ze zgromadzonego materiału dowodowego, chronologia zdarzeń kształtowała się następująco:

- […] lutego 2020 r. o godz. […] pracownik podmiotu przetwarzającego zrestartował jeden z serwerów używanych przez Spółkę. Powodem restartu były dane z monitoringu zasobów, które kazały sądzić, że serwer nie funkcjonuje optymalnie. Po restarcie podmiot przetwarzający nie zweryfikował prawidłowości konfiguracji zabezpieczeń. Wskazana data jest właściwą dla czasu zaistnienia naruszenia. W zgłoszeniu wstępnym i uzupełniającym Spółka nie miała wiedzy o dokładnych okolicznościach zdarzenia. Informacja ta została przekazana przez Spółkę w piśmie z […] marca 2020 r. po analizie wykonanej […] marca 2020 r. przez podmiot przetwarzający.
- […] marca 2020 r. o godz. […] Spółka otrzymała pierwszy sygnał o nieprawidłowości od niezależnego konsultanta w zakresie cyberbezpieczeństwa – […]. W wiadomości e-mail, sporządzonej w języku angielskim, skierowanej zarówno na główny adres e-mail Spółki oraz adres e-mail inspektora ochrony danych, badacz ten wskazał, że odkrył serwer z publicznie dostępnymi danymi klientów Spółki korzystających z witryny internetowej moneyman.pl. Przedmiotowa wiadomość stanowi załącznik nr […] do pisma Spółki z […] marca 2020 r.
- […] marca 2020 r. inspektor ochrony danych przesłał ww. wiadomość m.in. do dyrektora ds. finansów Spółki wraz z zapytaniem o kontakt do obsługi IT Spółki – IDFT. Dyrektor ds. finansów Spółki tego samego dnia przesłał ww. wiadomość do dyrektora IDFT opatrując ją komentarzem sugerującym, że może to być próba wyłudzenia poufnych informacji. Kopię tej wiadomości otrzymał m.in. dyrektor operacyjny Spółki. Działania dyrektora ds. finansów Spółki, zdaniem administratora, zmierzały do ustalenia, czy otrzymana informacja jest wiarygodna oraz czy udzielenie odpowiedzi nie zagraża bezpieczeństwu zasobów informatycznych Spółki.
- […] marca 2020 r. dyrektor ds. finansów Spółki ponownie zwrócił się do dyrektora IDFT w celu ustalenia, czy przekazana wiadomość została zweryfikowana. Tego samego dnia IDFT dokonała restartu serwera, jednak jego konfiguracja uwzględniająca prawidłowe zabezpieczenie środowiska była nadal nieprawidłowa.
- […] marca 2020 r. nieustalona osoba trzecia dokonała pobrania i usunięcia bazy danych Spółki pozostawiając informację z żądaniem uiszczenia okupu.
- […] marca 2020 r. o godz. […], za pomocą wiadomości e-mail, do Spółki zwrócił się redaktor portalu zaufanatrzeciastrona.pl wskazując na przedmiotowe naruszenie ochrony danych osobowych oraz adres IP serwera, którego naruszenie dotyczy. Jeszcze tego samego dnia informacja ta została przekazana m.in. do dyrektora ds. finansów Spółki.
- […] marca 2020 r. dyrektor ds. finansów Spółki przekazał ww. wiadomość dyrektorowi IDFT oraz Prezesowi Zarządu Spółki.
- […] marca 2020 r. o godz. […], dyrektor ds. finansów Spółki otrzymał wiadomość e-mail (stanowiącą załącznik do pisma Spółki z […] czerwca 2020 r.) od dyrektora IDFT z informacją o zidentyfikowaniu problemu oraz zaznaczył, że wcześniej podmiot ten nie miał do czynienia z taką sytuacją. Pracownicy IDFT ustalili, że do naruszenia poufności danych osobowych przetwarzanych na serwerze Spółki doszło w wyniku nieprawidłowej konfiguracji zapory sieciowej po restarcie serwera, tj. jeden z portów pozostawał otwarty. Potwierdzono nieuprawnione pobranie danych, ustalono skalę naruszenia oraz podjęto działania zaradcze, tj. m.in. przywrócono prawidłową konfigurację serwera (zamknięcie portu) oraz dokonano resetu haseł użytkowników portalu moneyman.pl. Spółka dokonała również weryfikacji wszystkich używanych przez nią serwerów, celem ustalenia, czy przetwarzane na tych serwerach dane są bezpieczne. Weryfikacja wykazała, że niebezpieczeństwo takie, w szczególności w zakresie nieuprawnionego dostępu, Spółce nie zagraża. Tego samego dnia Spółka dokonała wstępnego zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych.
- […] marca 2020 r. Spółka dokonała ponownej weryfikacji wszystkich używanych serwerów. Wnioski z weryfikacji były tożsame z tymi z […] marca 2020 r.
- […] marca 2020 r. Spółka skierowała do Prokuratury Okręgowej w Warszawie zawiadomienie o podejrzeniu popełnienia przestępstwa przez nieznanego sprawcę w związku ze zdarzeniem z […] marca 2020 r. (sygn. akt […]).

W kontekście zawiadomienia osób, których dane dotyczą, Spółka wskazała, że w dniach […] marca 2020 r. wysłała sms o treści: „[o]dzyskiwanie hasła do MoneyMan zakończyło się sukcesem. Nowe hasło to (…)", wskazując tym samym treść nowego hasła. W dniu […] marca 2020 r. rozesłała wiadomości e-mail do użytkowników o tożsamej treści. Kolejną wiadomość e-mail zawierającą pełną treść zawiadomienia z zakresem informacji wskazanych w art. 34 ust. 2 rozporządzenia 2016/679 skierowała […] marca 2020 r. Wiadomością sms z […] marca 2020 r. skierowaną do osób, których dane dotyczą, Spółka poinformowała, że „(…) ostatnia zmiana hasła była przeprowadzona automatycznie i wynikała ze względów bezpieczeństwa. Więcej na stronie www.moneyman.pl (…)". […] marca 2020 r. Spółka na stronie głównej moneyman.pl zamieściła informacje o naruszeniu oraz utworzyła dedykowane zakładki, w których doprecyzowała informacje przekazane w wiadomości sms z […] marca 2020 r. oraz informacje dotyczące naruszenia ochrony danych osobowych. Do wyjaśnień dołączono stosowne zrzuty ekranu.

Spółka wyjaśniając skuteczność dotarcia zawiadomienia o naruszeniu do osób, których dane dotyczą, przedstawiła szczegółową tabelę będącą raportem z wykazem dat, kanałów, rodzaju informacji oraz danych dotyczących dotarcia wiadomości. Jak wskazano, z tabeli wynika, że jedynie 4% podmiotów mogło nie otrzymać informacji o naruszeniu przekazanych za pośrednictwem korespondencji e-mail.

Odnosząc się do skuteczności udzielania informacji osobom, których dane dotyczą za pomocą wskazanych w zawiadomieniach numeru telefonu oraz adresu e-mail, Spółka wyjaśniała, że oddelegowała dodatkowych pracowników do działu Call Center, poinformowała pracowników w jaki sposób należy prowadzić komunikację z osobami, których dane dotyczą, przygotowała dla nich odpowiedzi na podstawowe pytania zadawane przez klientów w związku z naruszeniem ochrony ich danych osobowych, wstrzymała na okres trzech dni telefony windykacyjne, celem ułatwienia kontaktu klientom oraz w dniu […] marca 2020 r. wstrzymała sprzedaż nowych pożyczek, aby zapewnić skuteczną obsługę klientów, których dotyczy naruszenie.

Jak wynika z przedłożonych wyjaśnień, w zgłoszeniu naruszenia Spółka wskazała, że przedmiotowa baza danych nie była główną bazą danych klientów i potencjalnych klientów Spółki. Spółka w piśmie z […] marca 2020 r. wyjaśniła, że w bazie znajdowały się dane klientów Spółki, którzy po […] stycznia 2018 r. w całości lub w części przeszli przez proces rejestracji. Ponadto doprecyzowała zakres kategorii danych. Baza ta, jak wskazuje Spółka, omyłkowo zawierała hasła użytkowników portalu MoneyMan.pl, które przechowywane były otwartym tekstem. W głównej (produkcyjnej) bazie danych, hasła przechowywane są w postaci niejawnej.

Pismem z dnia […] maja 2020 r. Prezes Urzędu Ochrony Danych Osobowych zawiadomił Spółkę o wszczęciu postępowania administracyjnego, którego przedmiotem jest możliwość naruszenia przez Spółkę, jako administratora danych, obowiązków wynikających z przepisów rozporządzenia 2016/679 w zakresie obowiązków wynikających z art. 5 ust. 1 lit. f, art. 24 ust. 1, art. 25 ust. 1, art. 28 ust. 1, art. 28 ust. 3 lit. h, art. 32 ust. 1, art. 32 ust. 2, art. 33 ust. 1 oraz art. 34 ust. 1. W zawiadomieniu tym Prezes UODO wezwał Spółkę do złożenia dodatkowych wyjaśnień, w tym m.in. do:

- wyjaśnienia dlaczego baza danych, której dotyczy przedmiotowe naruszenie, przechowywała omyłkowo również hasła użytkowników, otwartym tekstem i jaka była rola tej bazy danych skoro w głównej produkcyjnej bazie danych Spółki hasła są przechowywane w postaci zaszyfrowanej;
- wskazania jakie postępowania weryfikacyjne podmiotu przetwarzającego pod kątem spełnienia przez niego wymogów rozporządzenia 2016/679 przeprowadził administrator przed zawarciem umowy powierzenia przetwarzania danych, a także, czy Spółka realizowała prawo kontroli z art. 28 ust. 3 lit. h rozporządzenia 2016/679;
- doprecyzowania okoliczności związanych ze zdarzeniem, które doprowadziło do naruszenia ochrony danych osobowych.

W odpowiedzi na zawiadomienie o wszczęciu postępowania, pismem z […] czerwca 2020 r. Spółka wskazała, że głównym celem istnienia bazy danych dotkniętej naruszeniem było opracowanie i przetestowanie skryptu badającego zachowania użytkowników portalu moneyman.pl w trakcie oraz po zalogowaniu się do panelu klienta (analiza behawioralna). Wdrożenie takiej funkcjonalności miało na celu przyczynienie się do zwiększenia bezpieczeństwa danych i zminimalizowania ryzyka ataków, kradzieży tożsamości i wyłudzeń finansowych. Spółka wskazała, że z uwagi na roboczy charakter tej funkcjonalności oraz dostęp ograniczonej liczby osób, baza ta nie została w odpowiednim momencie zaszyfrowana. Podkreśliła przy tym, że docelowo zastosowane środki bezpieczeństwa powinny być tożsame z tymi stosowanymi w bazie głównej. Jak wynika z tych wyjaśnień, dane osobowe znajdujące się w bazie głównej (produkcyjnej) nie są objęte naruszeniem ochrony danych osobowych i mimo usunięcia danych […] marca 2020 r. administrator nadal dysponował danymi, które pozwoliły mu zawiadomić osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych.

Odnosząc się do weryfikacji podmiotu przetwarzającego pod kątem spełnienia przez niego wymogów rozporządzenia 2016/679, Spółka wskazała, że kierując się koniecznością zapewnienia prawidłowej i profesjonalnej konfiguracji serwerów, postanowiła powierzyć pełnienie tych zadań wyspecjalizowanemu podmiotowi jakim jest IDFT, kierując się m.in. jego dużym doświadczeniem w obsłudze podmiotów z sektora finansowego, wysokimi kwalifikacjami pracowników oraz kompleksowego podejścia w obsłudze klienta. W 2018 r. spółka IDFT została poddana audytowi pod kątem obsługi Spółki w związku z przepisami rozporządzenia 2016/679. Wyniki tego audytu stanowią załącznik do pisma z […] czerwca 2020 r. Spółka wskazała również, że IDFT zrealizowała zadania, o których mowa w ww. dokumencie. Odnosząc się do realizacji prawa kontroli z art. 28 ust. 3 lit. h rozporządzenia 2016/679, Spółka wskazała, że podmiot przetwarzający niezwłocznie udzielał administratorowi informacji na temat zdarzenia z […] lutego 2020 r., jak również na przestrzeni całego okresu obowiązywania umowy powierzenia regularnie odbywały się rozmowy telefoniczne, telekonferencje i wzajemne, bezpośrednie wizyty. Ponadto podmiot przetwarzający udzielił Spółce odpowiedzi na pytania w ramach szczegółowego kwestionariusza weryfikującego przestrzeganie postanowień umownych. Wypełniony kwestionariusz stanowi załącznik do pisma z […] czerwca 2020 r.

W piśmie z […] czerwca 2020 r. Spółka doprecyzowała, że IDFT stosował wobec serwera, którego naruszenie dotyczy, zaporę sieciową, która ma możliwość zdefiniowania polityk ochrony sieci, filtrowania ruchu, itp. Rozwiązanie to należałoby uznać za wystarczające do uchronienia bazy danych przed naruszeniem, gdyby jego funkcje ochronne nie zostały nieświadomie wyłączone w związku z ludzkim błędem dotyczącym uruchomienia nieodpowiedniego skryptu konfiguracyjnego. Jeden z nich ([…]) zawierał polecenie resetu zasad w celu dalszej konfiguracji manualnej, podczas gdy inny ([…]) nie wymagał żadnych dalszych kroków manualnych. Według informacji przekazanych przez podmiot przetwarzający osoba, która popełniła błąd, została wcześniej przeszkolona z zasad cyberbezpieczeństwa, a podobne zadania wykonywała regularnie od dłuższego czasu. Ponadto, ww. osobie znana była procedura restartu serwera, która w praktyce sprowadza się do zastosowania konkretnego skryptu, wedle polecenia przełożonego. W ramach działań mających na celu zminimalizowanie prawdopodobieństwa zaistnienia podobnego zdarzenia w przyszłości, zrezygnowano ze skryptów wymagających konfiguracji manualnej oraz zmodyfikowano procedurę resetu serwera, która została załączona do pisma z […] czerwca 2020 r.

W wyniku analizy informacji zawartych w odpowiedzi na pismo informujące o wszczęciu postępowania Prezes Urzędu Ochrony Danych Osobowych, pismem z […] września 2020 r., zwrócił się do Spółki o wyjaśnienie, czy audyt podmiotu przetwarzającego przeprowadzony w związku z wejściem w życie rozporządzenia 2016/679 obejmował procedury związane z uruchamianiem nowych serwerów, ich

konfigurowaniem, resetowaniem i ostateczną weryfikacją, czy środki techniczne i organizacyjne odpowiadają na zagrożenia dla przetwarzanych danych. W piśmie z […] czerwca 2020 r. Spółka wskazuje, że osoba, która dopuściła się błędu, podobne zadania wykonywała regularnie od dłuższego czasu, w związku z tym Prezes UODO wezwał Spółkę do wskazania również, czy dostrzegła ryzyka związane ze stosowanie procedur uruchamiania skryptów do konfiguracji zapory sieciowej.

Spółka w odpowiedzi z […] września 2020 r. wskazała, że procedury stosowania skryptów były także sprawdzane podczas przeprowadzonych co pół roku audytów wewnętrznych i oceniane jako adekwatne. Błędu ludzkiego, który spowodował naruszenie, nie sposób było przewidzieć i uniknąć pomimo uwzględnienia różnych czynników ryzyka. Jak wskazuje spółka normalnym scenariuszem postępowania było automatyczne uruchamianie skryptu, co zapewniało stosowanie wszystkich zabezpieczeń. Incydent wystąpił w związku z manualnym restartem serwera, gdzie predefiniowane ustawienia nie zostały uruchomione.

W tym stanie faktycznym Prezes Urzędu Ochrony Danych Osobowych zważył, co następuje.

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"). Konkretyzację tej zasady stanowią dalsze przepisy rozporządzenia.

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.

Zgodnie z art. 25 ust. 1 rozporządzenia 2016/679 zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania administrator wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych (uwzględnianie ochrony danych w fazie projektowania).

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 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, zgodnie z lit. b i d tego artykułu, powinny obejmować środki takie, jak zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania 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.

Zgodnie z brzmieniem art. 33 ust. 1 rozporządzenia 2016/679 w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Przepisy rozporządzenia 2016/679 zobowiązują zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. Z wyżej wymienionych przepisów, jak i motywu 87 rozporządzenia 2016/679 wynika ponadto, że rozporządzenie ustanowiło wymóg przyjęcia ww. środków, by od razu stwierdzić naruszenie ochrony danych osobowych. Ma to decydujące znaczenie dla ustalenia, czy w danym przypadku zachodzą obowiązki z art. 33 ust. 1 i art. 34 ust. 1 rozporządzenia 2016/679.

Obowiązek powiadomienia organu nadzorczego o naruszeniu i termin jego przekazania wiąże się z momentem, w którym administrator „stwierdzi" naruszenie ochrony danych osobowych. Grupa Robocza Art. 29, w wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, przyjętych 3 października 2017 r., ostatnio zmienionych i przyjętych 6 lutego 2018 r. (dalej: wytyczne dotyczące zgłaszania naruszeń), wskazuje, że administrator stwierdza naruszenie w momencie, w którym uzyskał wystarczającą dozę pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych. **Należy jednak tą kwestie rozpatrywać względem obowiązku administratora utrzymania zdolności do szybkiego i skutecznego stwierdzania wystąpienia wszelkich naruszeń aby zapewnić możliwość podjęcia stosownych działań.** W niektórych przypadkach ustalenie,

czy doszło do ujawnienia danych osobowych, może wymagać czasu. **W tym kontekście powinno się jednak położyć nacisk na szybkie zbadanie danego incydentu w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak – podjąć działania zaradcze i, w razie konieczności, zgłosić naruszenie.**

Należy więc przyjąć, jak wskazuje Grupa Robocza Art. 29 w wytycznych dotyczących zgłaszania naruszeń, że po otrzymaniu pierwszej informacji o potencjalnym naruszeniu ochrony danych osobowych, od osoby fizycznej, z innego źródła lub po samodzielnym wykryciu incydentu bezpieczeństwa, administrator może przeprowadzić krótkotrwałe postępowanie, aby ustalić, czy faktycznie doszło do danego naruszenia. O ile do momentu zakończenia tego postępowania nie można uznać, że administrator stwierdził wystąpienie naruszenia, o tyle należy oczekiwać, **że wstępne postępowanie powinno rozpocząć się możliwie jak najszybciej i doprowadzić do jak najszybszego ustalenia z wystarczającą dozą pewności, czy w danym przypadku faktycznie doszło do wystąpienia naruszenia,** następnie można przeprowadzić bardziej szczegółową analizę zdarzenia. Jednak w **przypadku jakichkolwiek wątpliwości, mając w szczególności na względzie charakter i zakres przetwarzanych danych oraz ryzyko wiążące się z ich np. przypadkowym udostępnieniem, administrator powinien zgłosić naruszenie organowi nadzorczemu, nawet jeśli taka ostrożność mogłaby się okazać nadmierna. W motywie 85 rozporządzenia 2016/679 wyraźnie stwierdzono, że jednym z powodów, dla których zgłasza się naruszenie, jest ograniczenie związanych z nim szkód dla osób fizycznych**.Statuują to przytoczone wyżej przepisy, które konkretyzują zasadę poufności z art. 5 ust. 1 lit. f rozporządzenia 2016/679, obligującą do przetwarzania danych osobowych w sposób zapewniający odpowiednie ich bezpieczeństwo. Jak wskazują wytyczne dotyczące zgłaszania naruszeń, podczas oceny ryzyka, które może powstać w wyniku naruszenia, administrator powinien uwzględnić wpływ naruszenia na prawa i wolności osób fizycznych i prawdopodobieństwo jego wystąpienia.

W wiadomości e-mail z […] marca 2020 r., otrzymanej przez Spółkę, przedstawiony został fragment informacji zawierający dane osobowe użytkownika witryny moneyman.pl, które zlokalizowane są, w ocenie nadawcy, w infrastrukturze informatycznej Spółki. Fragment ten stanowił częściowe odzwierciedlenie struktury kategorii danych wraz z ich wartościami. Wśród nich znajdował się m.in. numer PESEL, adres e-mail i identyfikator użytkownika. O ile w piśmie tym nadawca nie wskazał adresu IP serwera, którego nieprawidłowa konfiguracja doprowadziła do naruszenia ochrony danych osobowych, o tyle zdaniem Prezesa UODO administrator nie podjął się dokładnej analizy i uwzględnienia zawartych w tej wiadomości informacji sugerujących, że udostępniona może być cała baza danych klientów Spółki. Przyjęcie chociażby takiej perspektywy powinno uzmysłowić Spółce skalę potencjalnego naruszenia i negatywnych konsekwencji dla jej klientów, do jakich może dojść lub już doszło. Dysponowanie już ww. informacjami powinno stanowić impuls do próby uzyskania dodatkowych informacji od nadawcy z zachowaniem należytej ostrożności oraz podjęcia działań weryfikacyjnych również we własnym zakresie. Chociażby, czy wskazane informacje dotyczące tej jednej przykładowej osoby odnoszą się rzeczywiście do jednego z klientów Spółki i czy nie powinny być w związku z tym przyczyną do podjęcia bardziej zintensyfikowanych działań we współpracy z podmiotem przetwarzającym. Nieuprawnione ujawnienie zakresu danych osobowych (wskazanych w opisie stanu faktycznego), bez wątpienia może skutkować wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, których te dane dotyczą. W związku z powyższym, zapewnienie odpowiedniego bezpieczeństwa takim danym powinno być przedmiotem szczególnej troski administratora, a każdy sygnał o ewentualnych nieprawidłowościach przedmiotem wnikliwej analizy.

W ocenie Prezesa UODO, administrator, po otrzymaniu wiadomości z […] marca 2020 r. nie kierował się ww. zasadami. Wskazuje na to m.in. jej przekierowanie przez dyrektora ds. finansów Spółki do dyrektora IDFT z krótkim komentarzem poddającym w wątpliwość intencje nadawcy i wskazujące na tzw. „smart phishing". O ile słusznie Spółka niezwłocznie przekazała wiadomość podmiotowi przetwarzającemu i oparła swoje przekonanie o konieczności zawiadomienia organu nadzorczego dopiero po potwierdzeniu jej wiarygodności, o tyle ze zgromadzonego materiału dowodowego nie wynika, by administrator podejmował inne działania zmierzające do szybkiego i skutecznego stwierdzenia naruszenia, oprócz skierowania […] marca 2020 r. krótkiego pytania do dyrektora IDFT. Jeśli zaistniałyby okoliczności wskazujące, że informacji tej nie można szybko i skutecznie zweryfikować, mając na względzie ryzyko dla praw i wolności osób fizycznych, Spółka powinna bez zbędnej zwłoki zgłosić naruszenie organowi nadzorczemu.

Zwłoka, której zdaniem Prezesa UODO dopuścił się administrator między […] marca 2020 r. a […] marca 2020 r., kiedy to otrzymała kolejny sygnał o naruszeniu, doprowadziła do jego eskalacji. Podatność serwera wykryta […] marca 2020 r. przez nieznaną osobę skutkowała pobraniem danych osobowych 140 699 klientów Spółki, ich usunięcia oraz pozostawienia wiadomości z żądaniem uiszczenia okupu. Dopiero po przekazaniu […] marca 2020 r. wiadomości z […] marca 2020 r. dyrektorowi IDFT, w którym to wskazano na obowiązki prawne ciążące na Spółce odnośnie terminu zawiadomienia organu nadzorczego, zarówno Spółka, jak i podmiot przetwarzający podjęły zintensyfikowane działania weryfikacyjne i zaradcze. Jak wynika z wyjaśnień Spółki, dopiero […] marca 2020 r. zespół IT podmiotu przetwarzającego ustalił przyczyny problemu po tym, jak sprawdził wiadomość e-mail z […] marca 2020 r. Prowadzi to do oczywistego wniosku, że weryfikacja tej wiadomości zajęła około 10 dni. Ponadto, jak Spółka wskazała, dopiero od […] marca 2020 r. inspektor ochrony danych Spółki rozpoczął gromadzenie informacji o naruszeniu.

Mimo, że Spółka wielokrotnie w swoich wyjaśnieniach w pismach z […] marca 2020 r. i z […] czerwca 2020 r. powołuje się na fakt niezwłocznego udzielania informacji Spółce przez podmiot przetwarzający na temat poszczególnych zdarzeń, w tym z […] lutego 2020 r., o tyle ze zgromadzonego materiału wynika, że informacje te były udzielane w sposób zintensyfikowany i z inicjatywy Spółki dopiero po […] marca 2020 r.

Jak wynika z pisma z […] czerwca 2020 r. Spółka w przeszłości nie stwierdziła podobnych nieprawidłowości, które doprowadziły do naruszenia ochrony danych. Jednocześnie wskazała, że restart serwera, jako procedura standardowa, był wielokrotnie wykonywany. Również dyrektor IDFT w wiadomości e-mail z […] marca 2020 r. wskazał, że dotychczas tak poważne zdarzenia nie miały miejsca.

W ocenie Prezesa UODO brak zdarzeń o podobnym charakterze nie może jednak usypiać czujności administratora i usprawiedliwiać brak odpowiednich działań z jego strony między […] marca 2020 r. a […] marca 2020 r.

Brak szybkiej reakcji ze strony podmiotu przetwarzającego nie zdejmuje z administratora odpowiedzialności za stwierdzenie naruszenia ochrony danych osobowych, gdyż zdolność do wykrywania naruszeń, zaradzania im oraz ich terminowego zgłaszania powinna być postrzegana jako kluczowy element środków technicznych i organizacyjnych, w tym każdej polityki w zakresie bezpieczeństwa danych. Spółka mimo niezwłocznego przekazania sygnału o nieprawidłowościach podmiotowi przetwarzającemu, zdaniem Prezesa UODO, nie podjęła swoich działań w sposób odpowiedni. Okoliczności sprawy jednoznacznie wskazują na to, że administrator pobieżnie przeanalizował wiadomość z […] marca 2020 r., nie potraktował jej z należytą powagą i nie zobligował podmiotu przetwarzającego do tego samego. Podjęcie właściwej analizy i zintensyfikowanego kontaktu z podmiotem przetwarzającym już w dniu […] marca 2020 r., w którym to Spółka dowiedziała się o pierwszych nieprawidłowościach, w ocenie Prezesa UODO, pozwoliłyby stwierdzić naruszenie ochrony danych znacznie szybciej (tak jak to uczyniono po wiadomości otrzymanej od redaktora jednego z portali internetowych) i potencjalnie zminimalizować ryzyko dla praw i wolności klientów Spółki, w tym uniknąć zdarzenia, do którego doszło […] marca 2020 r.

W dokumencie przedstawionym przez Spółkę pt. „Procedura zgłaszania naruszenia ochrony danych osobowych", w pkt […] wskazano, że jego celem jest stworzenie mechanizmu zapewniającego terminowe zgłoszenie naruszenia ochrony danych osobowych. W pkt […] stanowiącym schemat powiadamiania o naruszeniu danych osobowych wskazano, że rolą inspektora ochrony danych jest analiza zdarzenia i stwierdzenie naruszenia oraz ocena ryzyka dla osób fizycznych. W pkt […] wskazana jest procedura analizy zdarzenia, w którym inspektor ochrony danych, jako koordynator, weryfikuje i analizuje zdarzenie, angażując wszystkie jednostki związane z potencjalnym naruszeniem ochrony danych. W pkt […] z kolei wskazano przykładowe katalogi zdarzeń podlegających obowiązkom z art. 33 i 34 rozporządzenia 2016/679. Poza tym elementami dokument zawiera wiele ogólnych stwierdzeń, które można wywieść wprost z przepisów rozporządzenia 2016/679.

Tak więc swoim postępowaniem, mimo świadomości, w wyniku jakich zdarzeń może dojść do naruszenia ochrony danych osobowych (w procedurze mowa np. o błędnym działaniu systemu informatycznego czy błędzie ludzkim), wiadomość z […] marca 2020 r. została przez Spółkę potraktowana bez należytej powagi i sprzecznie ze stawianym w ww. procedurze oraz przepisach rozporządzenia 2016/679 celem, jakim jest stworzenie mechanizmu zapewniającego terminowe zgłoszenie naruszenia ochrony danych osobowych. Świadczy o tym pytanie inspektora ochrony danych skierowane do jednego z pracowników i dyrektora ds. finansów Spółki o kontakt do zespołu IT podmiotu przetwarzającego oraz sugestia dyrektora ds. finansów Spółki w wiadomości do dyrektora IDFT, wskazująca na tzw. „smart phishing". Umowa powierzenia przetwarzania danych osobowych z dnia […] marca 2018 r. w kontekście naruszeń ochrony danych, jedynie w § […] zawiera sprecyzowane obowiązki IDFT w przypadku naruszenia ochrony danych osobowych, jednakże ich brzmienie i wykładnia zdaniem Prezesa UODO związana jest już ze stwierdzonym naruszeniem.

Zarówno wyjaśnienia Spółki, jak i przedstawione przez nią dokumenty, nie przedstawiają procedury stwierdzenia naruszenia. O ile procedura taka nie jest wprost wymagana przez żaden z przepisów rozporządzenia 2016/679, o tyle, jak wskazują wytyczne dotyczące naruszeń i jak wynika to z przepisów rozporządzenia 2016/679, administrator jest zobligowany do sprawnego i szybkiego stwierdzania naruszenia ochrony danych, a taka procedura może to w znaczący sposób ułatwić.

Z odpowiedzi na wezwanie do wskazania, w jaki sposób administrator dokonywał regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych w systemach informatycznych, których naruszenie dotyczy, również nie wynika, by wspomniana procedura dotycząca zgłaszania naruszeń była od dnia jej uchwalenia weryfikowana pod kątem jej skuteczności.

Wobec powyższego Spółka, dokonując oceny pierwszego sygnału o nieprawidłowościach, nie uwzględniła – w ocenie Prezesa UODO – ryzyka wiążącego się z przetwarzaniem danych osobowych wynikających z przypadkowego udostępnienia danych osobowych, co stanowi naruszenie art. 32 ust. 2 rozporządzenia 2016/679. Zebrany w toku niniejszego postępowania materiał dowodowy stanowi również podstawę do stwierdzenia, że Spółka nie wywiązała się z obowiązku zapewnienia przetwarzania danych osobowych w sposób zapewniający ich odpowiednie bezpieczeństwo od momentu, w którym uzyskała pierwszy sygnał o nieprawidłowościach, co stanowi naruszenie zasady poufności wyrażonej w art. 5 ust. 1 lit. f rozporządzenia 2016/679. Nie wdrożyła również odpowiednich środków technicznych i organizacyjnych mających na celu skuteczną realizację ww. zasady ochrony danych, co stanowi naruszenie art. 25 ust. 1 rozporządzenie 2016/679 oraz skuteczne i szybkie stwierdzenie naruszenia, co stanowi naruszenie art. 24 ust. 1 rozporządzenia 2016/679. Zdaniem Prezesa UODO Spółka nie dokonywała również regularnej oceny skuteczności tych środków, co stanowi naruszenie art. 32 ust. 1 lit. d rozporządzenia 2016/679. Tym samym między […] marca a […] marca 2020 r. swoim działaniem przyczyniła się do niezapewnienia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, co stanowi naruszenie art. 32 ust. 1 lit. b rozporządzenia 2016/679.

W związku z wyjaśnieniami odnoszącymi się do regularnego testowania, mierzenia i oceniania przez administratora skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych w systemach informatycznych, których naruszenie dotyczy, należy zwrócić uwagę, że z tych wyjaśnień również nie wynika, by Spółka pozyskując dane klientów serwisu moneyman.pl po […] stycznia 2018 r. wykazała zainteresowanie sposobem, w jaki przechowywane są hasła użytkowników w dodatkowej bazie, która jest przedmiotem naruszenia. Niezrozumiałym w ocenie Prezesa UODO jest stwierdzenie Spółki, że hasła użytkowników omyłkowo były przechowywane otwartym tekstem i z uwagi na roboczy charakter tej funkcjonalności oraz dostęp ograniczonej liczby osób, baza ta nie

została w odpowiednim momencie „zaszyfrowana". Jak wskazała Spółka w wyjaśnieniach z dnia […] marca 2020 r. i […] czerwca 2020 r. celem istnienia bazy danych dotkniętej naruszeniem było opracowanie i przetestowanie skryptu badającego zachowania użytkowników portalu moneyman.pl w trakcie oraz po zalogowaniu się do panelu klienta (analiza behawioralna).

Prezes UODO wskazuje, że przechowywanie haseł w systemach informatycznych w postaci niejawnej (np. poprzez zastosowanie funkcji skrótu, zwanej też haszowaniem) jest jednym z najczęściej spotykanych środków mających zapewnić poufność hasła i ograniczyć jego znajomość wyłącznie do osoby, która się nim posługuje. Ogranicza się w ten sposób negatywne konsekwencje związane z potencjalnym ryzykiem wykorzystania takiego hasła przez osobę, która w sposób nieuprawniony, w powiązaniu z innymi informacjami, zapoznaje się z jej treścią. Osoba, która zna poświadczenia użytkownika dotyczące konkretnej usługi może uzyskać swobodny dostęp do jego konta. Należy zwrócić uwagę, że w przedmiotowej sprawie taka sytuacja mogła doprowadzić np. do oszustwa dotyczącego tożsamości, naruszenia dobrego imienia czy straty finansowej. Ponadto użytkownik mógł korzystać z takiej samej nazwy użytkownika (np. adres e-mail) i hasła w innych serwisach. Mając na względzie kategorie danych przetwarzanych przez Spółkę, zapewniając bezpieczeństwo tym danych, w szczególny sposób powinna brać takie okoliczności pod uwagę, gdyż krąg osób, które potencjalnie mogą być zainteresowane uzyskanymi poświadczeniami w celu ich wykorzystania niezgodnie z prawem, może być nieokreślony i rodzić negatywne konsekwencje dla praw i wolności osób, których dane dotyczą.

Mimo, że zastosowanie mechanizmu przechowywania hasła w postaci niejawnej nie eliminuje całkowicie prawdopodobieństwa, że osoba nieuprawniona odwróci ten proces i uzyska treść hasła, jego odpowiednie wykonanie powoduje, że ataki polegające na tzw. łamaniu haseł okazują się czasochłonne a nawet niepraktyczne. Celem takiego procesu jest m.in. uzyskanie odpowiedniego czasu na podjęcie działań zaradczych zarówno przez administratora, jak i osobę, której dane dotyczą, **zwłaszcza w przypadkach kiedy administrator nie stwierdzi naruszenia ochrony danych osobowych w czasie zbliżonym do jego faktycznego zaistnienia, co miało miejsce w sprawie będącej przedmiotem rozstrzygnięcia niniejszej decyzji.** Dlatego decydując się na takie rozwiązanie administrator powinien ocenić czy stosowane rozwiązania rzeczywiście spełnią swoją rolę. O ile Spółka słusznie w piśmie z […] września 2020 r. wskazuje, że relacja z podmiotem przetwarzającym nie oznacza obowiązku ciągłego monitorowania stosowanych rozwiązań, o tyle zdaniem Prezesa UODO istotnym jest by administrator w ramach realizacji obowiązków wynikających z rozporządzenia 2016/679 dokonywał cyklicznej weryfikacji, czy w używanych rozwiązaniach technicznych i organizacyjnych nie stwierdzono słabości mogących wpłynąć na ryzyko naruszenia praw lub wolności osób, których dane dotyczą, a fakt przetwarzania danych przez podmiot przetwarzający tej odpowiedzialności z administratora nie zdejmuje. **Zdaniem Prezesa UODO stanowi to o naruszeniu przez Spółkę art. 25 ust. 1 rozporządzenia 2016/679. Należy wskazać, że adresatem art. 25 ust. 1 rozporządzenia 2016/679 jest wyłącznie administrator, na którym ciąży obowiązek zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania wdrożenia odpowiednich środki technicznych i organizacyjnych, takich jak np. pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych.** Należy podkreślić, że koncepcja wynikająca z tego przepisu opiera się na proaktywnym i prewencyjnym podejściu administratora polegającym na zapewnianiu bezpieczeństwa danym osobowym na każdym etapie. Przyjęcie takich rozwiązań przez unijnego prawodawcę ma na celu wzmocnienie zasady poufności wyrażonej w art. 5 ust. 1 lit. f rozporządzenia 2016/679, tak byzapewnić przetwarzanym danym niezbędne, odpowiadające ryzykom związanym z ich przetwarzaniem, bezpieczeństwo. **Brak działań administratora w tym zakresie stanowi również o naruszeniu art. 24 ust. 1, art. 32 ust. 1 lit. d oraz art. 32 ust. 2 rozporządzenia 2016/679 poprzez brak uwzględnienia ryzyka związanego z przetwarzaniem haseł użytkowników w postaci jawnej, co w przypadku nie zastosowania innych środków technicznych i organizacyjnych mających na celu zapewnienie bezpiecznego przetwarzania, zgodnie z ww. przepisami rozporządzenia 2016/679, stanowi o narażeniu osób, których dane dotyczą, na zwiększenie ryzyka naruszenia praw lub wolności osób fizycznych w razie zaistnienia naruszenia poufności przetwarzanych danych.**

W toku postępowania administracyjnego, mimo stwierdzonych przez Prezesa UODO nieprawidłowości, które miały wpływ na naruszenie ochrony danych i jego spóźnione stwierdzenie, Prezes UODO nie dopatrzył się naruszenia art. 33 ust. 1 rozporządzenia 2016/679. Treść tego przepisu obliguje administratora do zawiadomienia organu nadzorczego o naruszeniu ochrony danych osobowych po spełnieniu dwóch kumulatywnych przesłanek – następuje stwierdzenie naruszenia, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.Jak już Prezes UODO niejednokrotnie wskazał w niniejszej decyzji, zgodnie z motywem 87 rozporządzenia 2016/679, wykładni przepisów rozporządzenia 2016/679 należy dokonywać m.in. przez pryzmat zdolności administratora do sprawnego i szybkiego stwierdzania naruszenia ochrony danych osobowych za pomocą stosowanych środków technicznych i organizacyjnych. Tak więc z tego tytułu stwierdzono naruszenie obowiązków nałożonych na Spółkę. **W konsekwencji Prezes UODO umorzył postępowanie administracyjne w zakresie naruszenia art. 33 ust. 1 rozporządzenia 2016/679, co tym samym nie stanowi podstawy wymiaru administracyjnej kary pieniężnej.**

Zgodnie z brzmieniem art. 34 ust. 1 rozporządzenia 2016/679, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Ponownie należy wskazać na wytyczne dotyczące zgłaszania naruszeń, które wskazują, że zawiadamiając osoby o naruszeniu ochrony danych, administrator powinien zachować w tej kwestii przejrzystość i przekazać informacje w sposób sprawny i terminowy. Analizując znaczenie określenia „bez zbędnej zwłoki" na gruncie tego przepisu należy przyjąć, że początkiem terminu na zawiadomienie osób, których dane dotyczą jest moment stwierdzenia naruszenia. Spółka, jak już wskazano w niniejszej decyzji, z opóźnieniem stwierdziła naruszenie […] marca 2020 r., co nie zdejmuje z niej odpowiedzialności za ryzyko naruszenia praw lub wolności osób, których dane dotyczą, powstałe w wyniku opóźnienia stwierdzenia naruszenia. Jednakże od razu po spóźnionym stwierdzeniu, Spółka z pomocą podmiotu przetwarzającego, rozpoczęła proces resetowania haseł użytkowników i podjęła wszelkie niezbędne działania mające na celu sprawne

i terminowe zawiadomienie osób, których dane dotyczą, w tym wykorzystała dostępne kanały informacyjne i w sposób wyczerpujący wykazała skuteczność dostarczenia zawiadomień. **W konsekwencji Prezes UODO umorzył postępowanie administracyjne w zakresie naruszenia art. 34 ust. 1 rozporządzenia 2016/679, co tym samym nie stanowi podstawy wymiaru administracyjnej kary pieniężnej.**

Zgodnie z brzmieniem art. 28 ust. 1 rozporządzenia 2016/679, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia 2016/679 i chroniło prawa osób, których dane dotyczą. Ponadto, zgodnie z ust. 3 lit. h tego artykułu, administrator posiada uprawnienia w zakresie uzyskania od podmiotu przetwarzającego wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 oraz posiada uprawnienie do przeprowadzania audytów, w tym inspekcji.

Z ww. przeprowadzonej analizy wynika, że Spółce należy postawić zarzuty niedopełnienia obowiązków wynikających z zapisów 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 2016/679. Nie sposób jednak zgodzić się ze stanowiskiem Spółki, że jej ewentualna odpowiedzialność, jako administratora, powinna być rozpatrywana jedynie w kontekście art. 28 ust. 1 rozporządzenia 2016/679 i odpowiedzi na pytanie, czy gwarancje udzielone administratorowi przez podmiot przetwarzający były wystarczające, aby uzasadnić skorzystanie z jego usług. Oceny tej rzecz jasna, jak wskazuje również Spółka, nie można dokonać jedynie z perspektywy samego incydentu, ale z perspektywy możliwości przewidzenia jego wystąpienia oraz możliwości rozsądnego stwierdzenia jeszcze przed wystąpieniem incydentu, że gwarancje nie są wystarczające i należy skorzystać z usług innych ekspertów IT. Słusznie również Spółka wskazuje, że art. 28 ust. 1 rozporządzenia 2016/679 wymaga korzystania z podmiotów przetwarzających zapewniających odpowiednie gwarancje zgodności, nie zaś ciągłego monitorowania stosowanych przez ten podmiot rozwiązań.

W pismach z […] marca, […] czerwca i […] września 2020 r. Spółka przedłożyła obszerne wyjaśnienia oraz liczne dokumenty, które regulują relację zachodzącą między ID Finance Sp. z o.o. w likwidacji a IDFT. Z punktu widzenia zapisów art. 28 ust. 1 i art. 28 ust. 3 lit. h rozporządzenia 2016/679 Prezes Urzędu Ochrony Danych Osobowych, w zgromadzonym materiale dowodowym, nie dopatrzył się okoliczności, które pozwoliłyby stwierdzić, że IDFT nie zapewniał wystarczających gwarancji dla bezpieczeństwa danych osobowych oraz nie udostępniał administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 bądź uniemożliwiał Spółce przeprowadzanie audytów, w tym inspekcji. **W konsekwencji Prezes UODO umorzył postępowanie administracyjne w zakresie naruszenia art. 28 ust. 1 i art. 28 ust. 3 lit. h rozporządzenia 2016/679, co tym samym nie stanowi podstawy wymiaru administracyjnej kary pieniężnej.**

Mając na uwadze powyższe ustalenia, Prezes Urzędu Ochrony Danych Osobowych, korzystając z przysługującego mu uprawnienia określonego w art. 58 ust. 2 lit. i rozporządzenia 2016/679, zgodnie z którym 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, mając na względzie okoliczności ustalone w przedmiotowym postępowaniu stwierdził, iż w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na Spółkę administracyjnej kary pieniężnej.

Decydując o nałożeniu na Spółkę administracyjnej kary pieniężnej, a także określając jej wysokość, Prezes UODO – stosownie do treści art. 83 ust. 2 lit. a-k rozporządzenia 2016/679 – wziął pod uwagę następujące okoliczności sprawy, wpływające obciążająco i mające wpływ na wymiar nałożonej kary finansowej:

1. **Charakter i waga naruszenia przy uwzględnieniu liczby poszkodowanych osób (art. 83 ust. 2 lit. a rozporządzenia 2016/679)** – przy wymierzaniu kary istotne znaczenie miała okoliczność, że liczba osób dotkniętych naruszeniem wynosi 140 699 (doprecyzowana w zgłoszeniu uzupełniającym z […] marca 2020 r.). Ponadto, Prezes UODO wziął pod uwagę, że zdarzenie z […] marca 2020 r. spowodowało wysokie ryzyko wystąpienia negatywnych skutków w przyszłości dla osób, których dane dotyczą, wynikających z szerokiego zakresu danych objętych naruszeniem, dużej liczby podmiotów danych oraz niewątpliwej złej woli osoby, która w sposób nieuprawniony uzyskała dostęp do danych, a także dużą skalę i profesjonalny charakter przetwarzania danych przez Spółkę. Podkreślić należy, że w stosunku do ww. 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 podjęły działania skutkujące wystąpieniem przedmiotowego naruszenia ochrony danych osobowych. Osoby, których dane dotyczą, mogą więc doznać szkody majątkowej, a już samo naruszenie poufności danych stanowi również szkodę niemajątkową (krzywdę). Podmiot danych może bowiem co najmniej odczuwać obawę przed utratą kontroli nad swoimi danymi osobowymi, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, czy wreszcie przed stratą finansową.
2. **Czas trwania naruszenia (art. 83 ust. 2 lit. a rozporządzenia 2016/679)** – zgromadzony materiał dowodowy pozwolił Prezesowi UODO stwierdzić, że Spółka nie podejmowała odpowiednich działań mających na celu sprawne i szybkie stwierdzenie naruszenia, co skutkowało potwierdzeniem nieprawidłowości przekazanych […] marca 2020 r. dopiero po około 10 dniach. Zwłoka, której dopuściła się Spółka ma istotny wpływ na wysokość nałożonej przez Prezesa UODO kary, gdyż jak wskazano w uzasadnieniu, podjęcie właściwej, rzetelnej analizy i zintensyfikowanie kontaktu z podmiotem przetwarzającym już w dniu […] marca 2020 r., w którym to Spółka dowiedziała się o pierwszych nieprawidłowościach, zdaniem Prezesa UODO, pozwoliłyby stwierdzić naruszenie ochrony danych znacznie szybciej (tak jak to uczyniono po wiadomości otrzymanej od redaktora jednego z portali internetowych) i potencjalnie zminimalizować ryzyko dla praw i wolności klientów Spółki, w tym uniknąć zdarzenia, do którego doszło […] marca 2020 r.

Jednocześnie wskazać należy, że okres trwania naruszenia polegającego na braku wdrożenia odpowiednich środków organizacyjnych i technicznych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, tj. procedur pozwalających na szybkie stwierdzenie naruszenia oraz gwarantujących regularną ocenę wdrożonych środków bezpieczeństwa, należy liczyć od momentu wprowadzenia przez Spółkę procedury zgłaszania naruszeń ochrony danych osobowych, tj. od […] maja 2018 r. Natomiast w zakresie naruszenia obejmującego brak uwzględnienia ryzyka związanego z przetwarzaniem haseł użytkowników w postaci jawnej, co w przypadku nie zastosowania innych środków technicznych i organizacyjnych mających na celu zapewnienie bezpiecznego przetwarzania, zgodnie z rozporządzeniem 2016/679, stanowi o narażeniu osób, których dane dotyczą, na zwiększenie ryzyka naruszenia praw lub wolności osób fizycznych w razie zaistnienia naruszenia poufności przetwarzanych danych, okres ten należy liczyć od […] stycznia 2018 r., tj. od dnia, w którym klienci Spółki w całości lub w części przeszli przez proces rejestracji w serwisie maneyman.pl.

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

Biorąc pod uwagę ustalenia w sprawie będącej przedmiotem rozstrzygnięcia niniejszej decyzji należy stwierdzić, że Spółka dopuściła się rażącego zaniedbania skutkującego naruszeniem poufności danych, do którego doszło […] marca 2020 r. Tak więc stanowi to istotną okoliczność wpływającą obciążająco na wysokość kary administracyjnej.

4. **Kategorie danych osobowych, których dotyczyło naruszenie ochrony danych osobowych (art. 83 ust. 2 lit. g rozporządzenia 2016/679)** - dane klientów Spółki, którzy po […] stycznia 2018 r. w całości lub w części przeszli przez proces rejestracji. Zakres danych stanowiących przedmiot naruszenia (doprecyzowany w piśmie z […] marca 2020 r.) jest następujący: imię i nazwisko, poziom wykształcenia, adres e-mail, dane dotyczące zatrudnienia, adres e-mail osoby, której klient chce polecić pożyczkę, dane dotyczące zarobków, dane dotyczące stanu cywilnego, numer telefonu (stacjonarnego, komórkowego, wcześniej używanego numeru telefonu), numer PESEL, narodowość, numer NIP, hasło (omyłkowo, jak wskazuje Spółka, przechowywane otwartym tekstem), miejsce urodzenia, adres korespondencyjny, adres zameldowania, numer telefonu do miejsca pracy oraz numer rachunku bankowego. Dane te nie należą do szczególnych kategorii danych osobowych, o których mowa w art. 9 rozporządzenia 2016/679, podlegających ze względu na swój wrażliwy charakter szczególnej ochronie. Jednakże ich bardzo szeroki zakres stanowi istotną okoliczność wpływającą obciążająco na wysokość kary administracyjnej.

5. **Wysoki stopień odpowiedzialności administratora (art. 83 ust. 2 lit. d rozporządzenia 2016/679)** – Biorąc pod uwagę, że to na administratorze ciąży prawny obowiązek sprawnego i terminowego stwierdzenia naruszenia oraz w określonych sytuacjach niezwłocznego zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, ustalenia dokonane przez Prezesa Urzędu Ochrony Danych Osobowych pozwalają na stwierdzenie, że Spółka nie wdrożyła odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych klientów w sytuacjach, w których otrzymuje pierwszy sygnał o nieprawidłowościach w przetwarzaniu danych osobowych, których jest administratorem.

Żadnego wpływu na fakt nałożenia, jak i sam wymiar administracyjnej kary pieniężnejnie miały inne, wskazane w art. 83 ust. 2 rozporządzenia 2016/679, okoliczności:

1. Działania podjęte przez Spółkę w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą (art. 83 ust. 2 lit. c rozporządzenia 2016/679) – Spółka dopełniła wobec osób, których dane pozyskane zostały przez osobę nieuprawnioną, obowiązku zawiadomienia o naruszeniu ochrony ich danych osobowych, o którym mowa w art. 34 rozporządzenia 2016/679. Nie podjęła jednak żadnych dodatkowych (wykraczających poza obowiązek prawny) działań mających na celu złagodzenie czy też wynagrodzenie krzywdy poniesionej przez osoby dotknięte naruszeniem.
2. Sposób w jaki organ nadzorczy dowiedział się o naruszeniu (art. 83 ust. 2 lit. h rozporządzenia 2016/679) – naruszenie ochrony danych osobowych zgłoszone zostało Prezesowi UODO przez Spółkę, co stanowi wypełnienie przez Spółkę ciążącego na niej obowiązku, o którym mowa w art. 33 rozporządzenia 2016/679.
3. Spółka nie stosuje zatwierdzonych kodeksów postępowania na mocy art. 40 rozporządzenia 2016/679 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 rozporządzenia 2016/679.
4. W tej samej sprawie nie zostały wcześniej zastosowane wobec Spółki środki, o których mowa w art. 58 ust. 2 rozporządzenia 2016/679.
5. Brak jest dowodów wskazujących na uzyskanie przez Spółkę korzyści finansowych, jak i powodujących uniknięcie strat w związku z naruszeniem.
6. Dobra współpraca ze strony Spółki, która w wyznaczonym terminie przesyłała wyjaśnienia i udzielała wyczerpujących odpowiedzi.

Uwzględniając wszystkie omówione wyżej okoliczności, Prezes Urzędu Ochrony Danych Osobowych uznał, iż nałożenie administracyjnej kary pieniężnej na Spółkę jest konieczne i uzasadnione wagą oraz charakterem i zakresem dokonanych przez Spółkę naruszeń.

Odnosząc się do wysokości wymierzonej Spółce 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. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b i lit. d oraz art. 32 ust. 2) zastosowanie znajdzie zarówno art. 83 ust. 4 lit. a rozporządzenia 2016/679, przewidujący m.in. za naruszenie obowiązków administratora, o których mowa w art. 25 i art. 32 rozporządzenia 2016/679, możliwość nałożenia administracyjnej kary pieniężnej w wysokości do 10 000 000 EUR (w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego), jak również art. 83 ust. 5 lit. a rozporządzenia 2016/679, zgodnie z którym naruszenia m.in. podstawowych zasad przetwarzania, o których mowa m.in. w art. 5 tego rozporządzenia, podlegają administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR (w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa).

Wobec powyższego, stosownie do treści art. 83 ust. 3 rozporządzenia 2016/679, Prezes Urzędu Ochrony Danych Osobowych określił całkowitą wysokość administracyjnej kary pieniężnej w kwocie nieprzekraczającej wysokości kary za najpoważniejsze naruszenie. W przedstawionym stanie faktycznym za najpoważniejsze należy uznać naruszenie przez Spółkę zasady poufności określonej w art. 5 ust. 1 lit. f rozporządzenia 2016/679. Przemawia za tym poważny charakter naruszenia oraz krąg osób nim dotkniętych (140 699 - stu czterdziestu tysięcy sześciuset dziewięćdziesięciu dziewięciu klientów Spółki, tj. osób, których danych administratorem jest Spółka).

Stosownie do treści art. 103 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), równowartość wyrażonych w euro kwot, o których mowa w art. 83 rozporządzenia 2016/679, oblicza się w złotych według średniego kursu euro ogłaszanego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, a w przypadku gdy w danym roku Narodowy Bank Polski nie ogłasza średniego kursu euro w dniu 28 stycznia - według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów Narodowego Banku Polskiego.

Mając powyższe na uwadze, Prezes Urzędu Ochrony Danych Osobowych, na podstawie art. 83 ust. 4 lit. a i art. 83 ust. 5 lit. a w związku z art. 83 ust. 3 rozporządzenia 2016/679 oraz w związku z art. 103 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, za naruszenia opisane w sentencji niniejszej decyzji, nałożył na Spółkę – stosując średni kurs euro z dnia 28 stycznia 2020 r. (1 EUR = 4,2794 PLN) – administracyjną karę pieniężną w kwocie 1.069.850,00PLN (co stanowi równowartość 250.000 EUR).

W ocenie Prezesa Urzędu Ochrony Danych Osobowych, 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 Ochrony Danych Osobowych nałożona na Spółkę kara będzie skuteczna, albowiem doprowadzi do stanu, w którym Spółka stosowała 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 Spółka od momentu zakończenia niniejszego postępowania będzie z najwyższą starannością podchodzić do wymogów stawianych przez przepisy o ochronie danych osobowych.

Zastosowana kara pieniężna jest również proporcjonalna do stwierdzonego naruszenia, w tym zwłaszcza jego wagi, kręgu dotkniętych nim osób fizycznych oraz ryzyka, jakie w związku z naruszeniem ponoszą. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych, nałożona na Spółkę kara pieniężna jest odpowiednia przy uwzględnieniu przychodów netto Spółki określonych za 2019 rok na poziomie 17,7 mln zł oraz za 2018 r. na poziomie 33,4 mln i nie będzie stanowiła nadmiernego dla niej obciążenia. Jak wynika z powyższych kwot, Spółka wykazuje co raz niższe przychody. Podkreślenia również wymaga, że Spółka podjęła kroki mające na celu zakończenie działalności poprzez podjęcie w dniu [...] czerwca 2020 r. jednomyślnej uchwały Nadzwyczajnego Zgromadzenia Wspólników spółki ID Finance Sp. z o.o. z siedzibą w Warszawie, w przedmiocie rozwiązania Spółki i powołania jej likwidatora. Jednocześnie jednak wskazać należy, że zgodnie z informacją odpowiadającą odpisowi aktualnemu z rejestru przedsiębiorców (numer KRS: "[...]"), według stanu na dzień 14 grudnia 2020 r., jedynym wspólnikiem Spółki jest IDFI, S.L., osoba prawna, spółka kapitałowa zarejestrowana wg prawa hiszpańskiego z siedzibą w B.

Wysokość kary została zatem 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 uiszczenia kary finansowej pociągnie za sobą negatywne następstwa, w postaci istotnego pogorszenia sytuacji finansowej Spółki. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych, Spółka powinna i jest w stanie ponieść konsekwencje swoich zaniedbań w sferze ochrony danych, stąd nałożenie kary w wysokości 1.069.850,00 PLN jest w pełni uzasadnione.

Administracyjna kara pieniężna spełni w tych konkretnych okolicznościach funkcję represyjną, jako że stanowić będzie odpowiedź na naruszenie przez Spółkę przepisów rozporządzenia 2016/679, ale i prewencyjną, czyli zapobiegnie naruszeniom przepisów o ochronie danych osobowych w przyszłości zarówno przez Spółkę, jak i innych administratorów danych.

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

2020-12-29

czynna w dni robocze od: 10:00-14:00

Techinfo

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
kancelaria@uodo.gov.pl
Godziny pracy: 8.00-16.00