Wpływ rozwoju technologicznego na odpowiedzialność odszkodowawczą

Impact of technological development on liability for damages

Charlotta Lendzion
absolwentka
Europejska Wyższa Szkoła Prawa i Administracji w Warszawie
ul. Okopowa 59
01-043 Warszawa
E: kontakt@kosmetykaprawo.pl
M: +48 537 022 007

WSTĘP

Rozwój technologiczny stał się powrzechny, podobnie jak korzystanie z zabiegów estetycznych. Działalność wielu gabinetów świadczących usługi w tym zakresie, oparta jest na programach przeznaczonych do obsługi klientów gabinetów kosmetologicznych. Właściciele salonów korzystają z rozwiązań technologicznych w różnych celach m.in do obsługi rezerwacji, sprzedaży usług, działań marketingowych itd. Należyta ochrona danych osobowych jest obowiązkiem osoby przetwarzającej dane osobowe, podobnie jak przekazanie szczegółowych informacji dotyczących przebiegu zabiegu.

Prezentacja tematyki odpowiedzialności odszkodowawczej w kontekście wykorzystywania technologicznych rozwiązań wynika z przyjęcia pewnych założeń związanych z ochroną danych osobowych w branży kosmetycznej (branży beauty). W artykule skupiono się na wykorzystywaniu różnego rodzaju aplikacji wykorzystywanych w celach marketingowych, organizacyjnych w odniesieniu do ochrony danych osobowych w kontekście odpowiedzialności odszkodowawczej. Każdy właściciel prowadzący firmę w branży beauty przetwarza dane osobowe, chociażby w kontekście rezerwacji czy kontaktu z klientem, dlatego dokumentacja dotycząca klientów powinna spełniać pełen zakres wymogów wskazanych w Rozporządzeniu o ochronie danych osobowych (RODO) oraz podstawowe zasady wymagane przez obowiązujące przepisy prawa. Nie realizując ustawowego obowiązku w tym zakresie naraża się nie tylko na odpowiedzialność administracyjną wskazaną przez RODO, ale również odpowiedzialność odszkodowawczą wobec klienta, którego dane zostały przetwarzane bez jego zgody.

» 330

STRESZCZENIE

W dobie intensywnego rozwoju technologicznego oraz komputeryzacji wdrażane są coraz nowsze narzędzia do pracy na wielu płaszczyznach rozwoju firm. Na tym tle, szczególnie ważna jest problematyka ochrony danych osobowych.

Nieodpowiednie wdrożenie i przestrzeganie przepisów w tym zakresie może wpływać nie tylko na odpowiedzialność administracyjną, ale również odszkodowawczą.

Celem niniejszego artykułu było omówienie zarysu zagrożeń wynikających z wykorzystywania technologii w świetle Rozporządzenia o ochronie danych osobowych (RODO) oraz wskazanie odpowiedzialności odszkodowawczej z tego wynikającej.

Osoby świadczące usługi w zakresie szeroko pojętej kosmetologii powinny w szczególny sposób zadbać o dane osobowe klientów, albowiem w tej branży przetwarzanych jest wiele danych wrażliwych.

Słowa kluczowe: ochrona danych osobowych, odpowiedzialność odszkodowawcza, prawo, technologie, biznes, uroda

ABSTRACT

In the era of intensive technological development and computerization new tools are being implemented to work on many levels of company development. Against this background the issue of personal data protection is particularly important.

Inadequate implementation and compliance with regulations in this regard may affect not only administrative responsibility but also damages.

The purpose of this article was to discuss the outline of threats arising from the use of technology in the light of the GDPR Regulation and the liability for damages arising therefrom.

Professionals providing services in the field of broadly defined cosmetology should take special care of clients' personal data, because this industry is particularly important from the perspective of processing sensitive data.

Keywords: *personal data protection, liability for damages, law, technologies, business, beauty*

otrzymano / received
12.03.2020
poprawiono / corrected
07.04.2020
zaakceptowano / accepted
08.05.2020

OCHRONA DANYCH OSOBOWYCH

Ochrona danych osobowych pełni coraz bardziej kluczową rolę, a to za sprawą (RODO) 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. Rozporządzenie to wprowadziło szereg wymagań jakie powinny przestrzegać podmioty wykorzystujące dane osobowe. Powszechność stosowania różnego rodzaju aplikacji, chmur obliczeniowych do przechowywania danych, czy też oprogramowania od zewnętrznych dostawców, sprawia, że zapanowanie nad danymi osobowymi staje się nie lada wyzwaniem.

Nie zmienia to jednak faktu, że przepisy mają zastosowanie do każdego z przedsiębiorców i każdy kto przetwarza dane, zobligowany jest do ich przetwarzania w granicach prawa. Brak należytej staranności i zabezpieczeń może być przyczyną do potencjalnego powództwa ze strony klienta, albowiem działalność osób wykonujących usługi beauty nie może naruszać podstawowych praw i wolności klientów, w szczególności prawa do ochrony danych osobowych. Należyta staranność, odpowiednie zabezpieczenia oraz prowadzenie biznesu zgodnie z wymogami prawnymi mają zminimalizować potencjalne ryzyko z tym związane. Dlatego bardzo istotne jest zwrócenie uwagi na to, czym jest odpowiedzialność odszkodowawcza w kontekście ochrony danych osobowych.

Można wyróżnić dwa rodzaje odpowiedzialności:
- odpowiedzialność na zasadzie winy oraz
- odpowiedzialność na zasadzie ryzyka.

Oczywiście istnieją jeszcze inne rodzaje odpowiedzialności, chociażby odpowiedzialność karna czy administracyjna, jednak w artykule skupiono się wyłącznie na odpowiedzialności cywilnej w kontekście naruszeń danych osobowych np. przy wycieku danych klientów.

Dane osobowe

Na potrzeby omawianego zagadnienia warto objaśnić w pierwszej kolejności czym są dane osobowe. Zgodnie z Rozporządzeniem – *„Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej*". Zatem w salonie beauty oczywiste jest korzystanie z danych osobowych – chociażby przy rezerwacji wizyty, czy wypełnianiu formularza wywiadu zdrowotnego [1].

Administrator danych

Drugą definicją, która wymaga poruszenia w tym artykule, jest definicja administratora danych. Zgodnie z treścią artykułu 4 ust. 7 i 8 Rozporządzenia – *„Administratorem danych jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania*". Zatem administratorem jest każdy kto przetwarza dane osobowe w związku z prowadzeniem działalności lub przetwarza je w celach innych niż przetwarzanie przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze [1].

Przetwarzanie

W połączeniu dwóch powyższych definicji dochodzi do czynności nazywanych „przetwarzaniem". Zgodnie z definicją Rozporządzenia – *„Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie"* [1].

Profilowanie

Omawiając zakres wykorzystywanej technologii nie można zapomnieć o definicji profilowania, które również pełni istotną rolę. Definicja w Rozporządzeniu brzmi – *„Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się"* [1].

OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA PRIVACY BY DESIGN/BY DEFAULT

Przechodząc do zagadnień wykorzystywania technologii i zakresu odpowiedzialności odszkodowawczej przy jej wykorzystywaniu, należy omówić technologiczne rozwiązania, które są wykorzystywane do prowadzenia firmy w branży beauty.

Mając na uwadze pogląd na technologię z szerszej perspektywy należy wskazać czym jest program komputerowy i czym jest chmura. Są to istotne zagadnienia, albowiem

pozwalają nie tylko poszerzyć zakres wiedzy i świadomości, ale również zwiększyć zakres badania ryzyka pod kątem przetwarzania danych.

Program komputerowy

Zgodnie z treścią dyrektywy 2009/24/WE pkt 7 – *„Przez pojęcie program komputerowy rozumie się programy w jakiejkolwiek formie, w tym programy zintegrowane ze sprzętem komputerowym; pojęcie to obejmuje również przygotowawcze prace projektowe prowadzące do rozwoju programu komputerowego z zastrzeżeniem, że charakter prac przygotowawczych jest taki, że program komputerowy może korzystać z nich na późniejszym etapie”*. Nie jest to jednak jedyna definicja programu komputerowego. Inna, wypracowana przez doktrynę wskazuje, że program komputerowy czy aplikacja jest *„efektem działalności intelektualnej twórcy w postaci konstrukcji językowej składającej się ze skończonego ciągu ściśle określonych instrukcji postępowania prowadzących do rozwiązania konkretnego zadania w skończonej liczbie kroków oraz zadań wyrażonych językiem programowania, dostarczających informacji o rodzaju i strukturze danych oraz określających obszar w pamięci komputera zarezerwowany dla zmiennych i postaci danych, jakie maja być przechowywane w tymże obszarze*”. Przekładając powyższe na przykłady z życia codziennego, programem komputerowym są m.in programy/aplikacje do rezerwacji wizyt w salonach beauty, może być to też strona internetowa, która w sposób zautomatyzowany kontaktuje się z klientami, sklep internetowy, aplikacja, która odpowiada na pytania (chatbot), programy obsługujące płatności, działania marketingowe np. mailingi, aplikacje mobilne skanujące dokumenty i zmieniające je na formę cyfrową, wszelkiego rodzaju inne aplikacje mobilne [2-4].

Chmura obliczeniowa (potocznie nazywana internetową)

Część osób korzystając z danych, nie tylko osobowych, ale wszelkich danych wykorzystywanych w swoim biznesie bardzo często korzysta z zewnętrznych przestrzeni pamięci tzw. chmury [2-4].

Chmury, według niektórych, to miejsca do przechowywania danych wykorzystywane wyłącznie przez duże korporacje. Jest to mit, albowiem część z nas być może nawet nie wie, że korzysta z chmur w postaci zewnętrznych dysków, miejsc do przechowywania danych, których dostawcami są np. Google, Dropbox czy iCloud. Dlaczego jest to istotne? Dlatego, że w przypadku wykorzystywania zewnętrznych chmur i przechowywania tam danych, osoba przetwarzająca/administrator powinna oszacować ryzyko związane z potencjalnym wyciekiem.

Rodzaje chmur internetowych

- Publiczne, z których korzystanie przeważnie jest darmowe. Są dostępne do użytku publicznego, są własnością dostawcy, który nimi zarządza. Korzystanie z takiej chmury przeważnie wiąże się z akceptacją regulaminu, który jest z góry narzucony, a użytkownik (osoba, która chce z niej korzystać) nie ma możliwości negocjowania warunków jej użytkowania zgodnie z własnymi potrzebami.
- Chmury prywatne, które przeznaczone są do wyłącznego użytku przez danego użytkownika (firmę) mogą być konfigurowane w zależności od potrzeb dla danego lub przez danego użytkownika. Są one nie tylko bezpieczne, ale przeważnie wiążą się z indywidualnymi warunkami, które elastycznie mogą być dopasowane do danego podmiotu (firmy, użytkownika).
- Chmury hybrydowe, które są połączeniem opcji publicznej z prywatną, a czasami również ze społecznościową. Składają się z dwóch lub większej ilości chmur [2, 4, 25].

Chmury w salonie beauty mogą być wykorzystywane w różny sposób np. do przechowywania danych osobowych klientów do celów marketingowych, czy też do przechowywania zdjęć, wysyłania dokumentów itd. Warto w tym miejscu wskazać, że usługi przetwarzania danych w chmurze mają charakter powierzenia czynności przetwarzania i może to być traktowane jako outsourcing. Dlatego też istotne jest to, aby w sposób należyty zabezpieczyć dane osobowe klientów, czy też tajemnicę przedsiębiorstwa np. poprzez odpowiednie szyfrowanie danych, choć uznaje się, że nawet szyfrowanie danych nie daje 100% gwarancji ochrony. Tym samym każdy salon beauty, który korzysta z chmury powinien oszacować ryzyko związane z bezpieczeństwem informacji, które tam się znajdują.

Na tym tle szczególnie wyraźnie przedstawia się problem odpowiedzialności odszkodowawczej administratora danych osobowych w sytuacji kiedy dojdzie do wycieku tych danych lub jeżeli te dane będą wykorzystywane w sposób nieadekwatny do celu, czy też bez zgody. Jak już wcześniej wskazano wszystkie czynności realizowane przez administratora (do których jest zobligowany Rozporządzeniem) będą weryfikowane w przypadku dojścia do zawinionego działania lub zaniechania przy przetwarzaniu danych [1].

Przedsiębiorcy dość często wykazują brak świadomości faktu, że są odpowiedzialni nie tylko za oprogramowanie czy stronę internetową, ale również wykorzystywane narzędzia w kontekście ochrony danych osobowych.

Zgodnie z treścią artykułu 25 Rozporządzenia ust. 1 i 2 – *„Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony*

danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego Rozporządzenia oraz chronić prawa osób, których dane dotyczą" [1].

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych" [1].

W kontekście rozważań wskazanego artykułu 25 Rozporządzenia wskazuje się na dwie istotne kwestie dotyczące przetwarzania danych. Już na etapie projektowania technologii m.in. stron internetowych – *privacy by design* oraz *privacy by default* wymuszany jest na wszystkich administratorach danych obowiązek uwzględnienia ochrony danych i prywatności na każdym etapie tworzenia oprogramowania i jego późniejszego wykorzystywania (np. wprowadzając produkty do sklepu internetowego) spełnienie wszelkich przesłanek Rozporządzenia [5].

Jednym słowem, osoba świadcząca usługi w branży beauty w chwili tworzenia własnej strony www lub innego oprogramowania, będzie zobowiązana do wprowadzenia rozwiązań mających na celu ochronę danych osobowych. Jednym z takich rozwiązań jest na przykład wprowadzenie odpowiednich zabezpieczeń przed przejęciem strony tzw. zhakowaniem.

W aspekcie stron internetowych, na pierwszy rzut przychodzą takie kwestie jak polityka prywatności, obowiązek informacyjny administratora danych, polityka plików cookie. Jeżeli podmiot korzysta z wtyczek społecznościowych np. „lubię to", Google Analytics, Disques, Instagram, Twitter i innych, wówczas należy wskazać, że dane osobowe są przekazywane również do tych podmiotów. Jeżeli podmiot korzysta z newslettera lub innych formularzy, niezbędne jest wstawienie odpowiednich checkboxów, w których użytkownik wyraża zgodę na przetwarzanie danych oraz potwierdza zapoznanie się z np. z polityką prywatności. Takich elementów jest znacznie więcej w zależności o tego jak rozbudowana jest strona internetowa czy aplikacja. Zgodność prawna w tym zakresie jest kluczowa na każdym etapie korzystania z danej technologii [1, 6].

O ile może wydawać się, że treść Rozporządzenia jest jasna i wymogi jakie są stawiane wytwórcom oprogramowania w tym zakresie, o tyle zmieni się kontekst jeżeli stronę internetową tworzy właściciel salonu kosmetycznego, albowiem to na nim w każdej sytuacji będzie spoczywała odpowiedzialność za poprawne i zgodne z prawem wdrożenie wymogów RODO. Za zewnętrzne aplikacje należy uznać takie, które udostępnione są głównie do bezpłatnego używania. Warto jednak wskazać, że jeżeli coś jest bezpłatne, to faktycznie oznacza, że użytkownicy płacą za to swoimi danymi.

W przeprowadzonej ankiecie wśród 150 przedsiębiorców dotyczącej znajomości regulaminów pobranych aplikacji na ich smartfony, tylko 9% zadeklarowała, że przeczytała regulamin. Warto wskazać, że w większości regulaminy są pisane w językach innych niż polski, a co za tym idzie większość osób nie czyta ich, tylko zatwierdza zapoznanie się z warunkami korzystania z aplikacji, a tym samym daje przyzwolenie na wykorzystywanie informacji zawartych w telefonie (zdjęcia, kamera, lista kontaktów itd.) [7].

Wszystko to wpływa na ochronę danych osobowych klientów i ma ogromne znaczenie w kontekście odpowiedzialności odszkodowawczej. Wykorzystując zewnętrzne aplikacje nie mamy wpływu na ich rozwój, testy, weryfikację zgodności prawnej, czy też ochronę danych osobowych w nich przechowywanych, a co za tym idzie, nie mamy żadnej kontroli nad tym co dzieje się z danymi klientów. Kontrola jest podstawowym elementem tego, aby odpowiednio chronić dane osobowe. Kontrola i ochrona, panowanie nad procesem przetwarzania to m.in wykazanie jednej z przesłanek należytej staranności, która w aspekcie odpowiedzialności odszkodowawczej będzie rozpatrywana przez sąd. Jeżeli nie potrafimy zagwarantować odpowiedniej ochrony danych, nie powinniśmy ich przetwarzać.

Oczywiście w dobie wykorzystywania zaawansowanych technologii informatycznych, tego typu wnioski mogą być uważane za zbyt ideologiczne, jednak w kontekście realnego zagrożenia jakim są czarne rynki sprzedaży danych osobowych czy kradzieże tożsamości, tego typu ryzyka są istotnym elementem, który powinien być brany pod uwagę przez każdego przedsiębiorcę i odpowiednio oszacowany w kontekście ryzyk.

Aplikacje pobrane na smartfon mogą mieć również istotny wpływ na inne aplikacje. Wielokrotnie w smartfonie użytkownicy pobierają pocztę swojego przedsiębiorstwa, przyjmują zlecenia usług kosmetycznych, a jednocześnie na tym samym smartfonie ściągają gry lub inne aplikacje rozrywkowe, które żądają dostępu do kontaktów, głośnika, kamery, albumu zdjęć czy też wymagają korzystania z systemu wykrywania lokalizacji. Wszystko po to, aby wykorzystywać dane znajdujące się w telefonie użytkownika do własnych celów.

Problem ochrony danych pojawia się w sytuacji kiedy udostępniamy dostęp do kontaktów zapisanych w telefonie zawierających dane osobowe klientów (imię, nazwisko, adres, e-mail, nr telefonu). Problem staje się większy, jeżeli klienci nie wyrażali zgody na przekazywanie danych osobowych innym podmiotom, a tym bardziej podmiotom spoza obszaru Unii Europejskiej.

Celowo wskazany został obszar poza UE, albowiem zapisanie danych osobowych w chmurze zewnętrznego podmiotu, który ma swoje serwery np. w Stanach Zjednoczonych, wyrażenie zgody aplikacji na dostęp do kontaktów w smartfonie, która również ma serwer na terenie

USA uznaje się za przekazywanie danych poza obszar UE i tego typu informacja powinna być przekazana klientowi, albowiem powinien on o tym wiedzieć. Nie informując go o tym fakcie, przedsiębiorca łamie przepisy Rozporządzenia oraz naraża się na odpowiedzialność nie tylko administracyjną, ale również odszkodowawczą [1, 8].

W sytuacji kiedy klient wniesie pozew przeciwko danemu przedsiębiorcy w zakresie odpowiedzialności odszkodowawczej w kontekście naruszenia danych osobowych, sąd ma prawo powiadomić Prezesa urzędu ochrony danych osobowych o możliwości wstąpienia do sprawy. W przypadku kiedy dojdzie do wycieku danych u osoby prowadzącej salon beauty, który to wyciek nie zostanie zgłoszony, a klient dowiedziawszy się o tym złoży pozew do sądu (nie do Urzędu Ochrony Danych Osobowych UODO), wówczas i tak sąd może powiadomić Prezesa UODO o całym zajściu.

Pozwany, czyli osoba prowadząca biznes beauty jest wówczas w dużo gorszej sytuacji procesowej z racji tego, że pojawią się ujemne skutki procesowe w postaci podejrzenia ukrycia całego zajścia. Co ważne, wydana przez Prezesa UODO decyzja o naruszeniu przepisów o ochronie danych osobowych jest wiążąca dla sądu – jeżeli UODO uzna, że doszło do naruszenia przepisów, sąd rozpoznający sprawę w postępowaniu cywilnym nie może orzec, że do naruszenia nie doszło. Biorąc pod uwagę stan doświadczenia życiowego może zdarzyć się tak, że sąd może zawiesić rozprawę do czasu ustalenia przez UODO czy do wycieku rzeczywiście doszło i kto ponosi za to winę [1, 9].

ODPOWIEDZIALNOŚĆ ODSZKODOWAWCZA ZA NARUSZENIE DANYCH OSOBOWYCH

Przepisy Rozporządzenia, a dokładniej artykuł 82, wskazuje na zakres prawa do odszkodowania w sytuacji, w której dojdzie do naruszenia danych. Jest to bardzo istotny artykuł, albowiem jest to *lex specialis*, czyli przepis szczególny w odniesieniu do zasad ogólnych przepisów Kodeksu cywilnego. Innymi słowy jest to artykuł szczególny, który ma pierwszeństwo przed Kodeksem cywilnym. Czytamy najpierw ten artykuł, a w dalszej interpretacji odnosimy się do ogólnych zasad Kodeksu cywilnego. Dlatego wartością dodaną w omawianej tematyce powinno być jego omówienie, albowiem będzie on kierunkowskazem do dalszej interpretacji w kontekście odpowiedzialności odszkodowawczej. Na tym tle szczególnie wyraźnie przedstawia się problem dokładnego zrozumienia czym jest odpowiedzialność na zasadzie winy (odpowiedzialność deliktowa) oraz na zasadzie ryzyka, unormowane w Kodeksie cywilnym, bo zrozumienie podstaw ułatwi zrozumienie zakresu odpowiedzialności wywodzonych w artykule 82 Rozporządzenia.

Kontekst odpowiedzialności należy rozpocząć od objaśnienia czym jest odpowiedzialność na zasadzie winy i na zasadzie ryzyka, albowiem te dwie kwestie są bardzo istotne w omawianym temacie.

Rodzaje odpowiedzialności odszkodowawczej

Odpowiedzialność na zasadzie winy opisana jest w artykule 415 Kodeksu cywilnego – *„Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia*". Z tej niewielkiej treści dowiadujemy się, że każdy kto wyrządzi komukolwiek, jakąkolwiek szkodę zobowiązany jest ją naprawić, ale dowiadujemy się również, że musi ponosić „winę" za wyrządzenie szkody. Wina w prawie cywilnym zachodzi wtedy, kiedy sprawcy szkody można postawić obiektywny oraz subiektywny zarzut niewłaściwości zachowania. Innymi słowy, obiektywność rozpatrywania winy będzie stanowiła tzw. bezprawność, która ma na celu złe działanie lub zaniechania sprawcy w odniesieniu do porządku prawnego, np. naruszenie konkretnego przepisu prawnego, zasad współżycia społecznego lub innych norm powszechnie stosowanych w społeczeństwie.

Odpowiedzialność na zasadzie ryzyka wskazuje artykuł 435 Kodeksu cywilnego – *„Prowadzący na własny rachunek przedsiębiorstwo lub zakład wprawiany w ruch za pomocą sił przyrody (pary, gazu, elektryczności, paliw płynnych itp.) ponosi odpowiedzialność za szkodę na osobie lub mieniu, wyrządzoną komukolwiek przez ruch przedsiębiorstwa lub zakładu, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy poszkodowanego lub osoby trzeciej, za którą nie ponosi odpowiedzialności"*. Ten rodzaj odpowiedzialności jest przypisany jako główny do osób, które jako profesjonaliści prowadzą biznes w branży beauty. Jak wskazuje powyższa treść omawianego artykułu, odpowiedzialność na zasadzie ryzyka jest odpowiedzialnością bardziej rygorystyczną, albowiem nie ma znaczenia czy doszło do winy sprawcy przy wyrządzeniu szkody, ale istotny jest czynnik obiektywny polegający na tym, że istotne jest to, że wystąpiła szkoda i że jest ona w związku przyczynowo-skutkowym z danym przedsiębiorstwem (zdarzeniem w nim). Należy jednak wskazać, że w porównaniu do odpowiedzialności na zasadzie winy, ten rodzaj odpowiedzialności ma możliwość uwolnienia się od odpowiedzialności właściciela salonu beauty w trzech przypadkach. Po pierwsze – szkoda musiała wystąpić na skutek siły wyższej, czyli czynników obiektywnie niezależnych od właściciela salonu. W drugim przypadku szkoda nastąpiła wyłączenie z winy poszkodowanego. Natomiast w trzecim przypadku jeżeli szkoda wystąpiła wyłącznie z winy osoby trzeciej, za którą właściciel salonu beauty nie ponosi odpowiedzialności. Te trzy przesłanki dają możliwość uwolnienia się od odpowiedzialności właściciela w przypadku wystąpienia szkody, jednak zaznaczając, że jeżeli będzie chciał się na nie powołać, będzie musiał udowodnić ich wystąpienie przed sądem.

Reasumując, należy wskazać, że w przypadku rozpatrywania odpowiedzialności właściciela salonu beauty w pierwszej kolejności rozpatrywany jest aspekt odpowiedzialności na zasadzie ryzyka, a w drugiej, jeżeli zakres szkody tego

wymaga lub przepisy na to wskazują również w kontekście winy. Nie zmienia to jednak faktu, że w kontekście rozpatrywania odpowiedzialności odszkodowawczej należy wskazać jej trzy podstawowe filary. Pierwszy to wystąpienie szkody, drugi dotyczy zdarzenia przez które szkoda wystąpiła, trzeci dotyczy związku przyczynowo-skutkowego (adekwatno-skutkowego) łączącego zdarzenie ze szkodą [1, 10-14].

SZKODA

Czym jest szkoda i jak należy ją rozumieć oraz udowodnić? Kodeks cywilny nie formułuje pojęcia szkody, dlatego też na potrzeby interpretacji w artykule odwołano się do dorobku doktryny. Słownik języka polskiego definiuje szkodę jako stratę materialną lub niematerialną, jednak z perspektywy prawnej warto wskazać, że zgodnie z doktryną, szkodę uznaje się za uszczerbek w dobrach, które są prawnie chronione. Uszczerbek ten może być majątkowy albo niemajątkowy w zależności czego on dotyczy. Może to być sytuacja, w której na podstawie wycieku danych osobowych z salonu beauty klientka dozna szkody. Przykładem takiego wycieku, który obrazuje potencjalne ryzyko związane z cyberatakami jest sytuacja, która miała miejsce u jednego szkockiego fryzjera. Hakerzy zablokowali bazę danych firmy fryzjerskiej i zagrozili usunięciem wszystkich danych. Zadeklarowali, że przywrócą dane firmy tylko wtedy, gdy fryzjer zapłaci 1000 Euro. Firma wpłaciła pieniądze hakerom (za pomocą Bitcoinów) ponieważ nie chciała stracić reputacji ani klientów. Sprawa jest aktualnie wyjaśniana. Nie zmienia to jednak faktu, że mniejsze firmy nie zgłaszają tego typu incydentów w obawie utraty klientów, reputacji, czy też nałożeniu ogromnych kar. Warto jednak podkreślić, że istota problemu leży w budowaniu świadomości korzystania z narzędzi technologicznych w taki sposób, aby dane osobowe nie były zagrożone [15].

Jak już wcześniej wskazano, szkoda może mieć odzwierciedlenie majątkowe, czyli mające pewną wartości wyrażoną wprost w pieniądzu. Przykładem takiej szkody może być sytuacja, w której hakerzy wykorzystają skradzione dane klientów do zaciągnięcia pożyczek. Szkoda niemajątkowa to szkoda, która dotyczy sfery niematerialnej czyli np. dóbr osobistych. Przykładem takiej szkody może być opublikowanie danych wrażliwych w sieci w skutek czego dojdzie do naruszenia dóbr osobistych.

Warto wskazać, że szkoda może uwzględniać straty, ale również korzyści, które ktoś mógłby otrzymać w przyszłości jeżeli do danej szkody by nie doszło, zgodnie z tezą wyroku Sądu Apelacyjnego w Białymstoku o sygnaturze I ACa 724/16 szkodą niemajątkową klienta może być również sam fakt nie wywiązania się przez administratora danych z obowiązku informacyjnego [13, 16, 17].

Oczywiście przykłady można mnożyć, wszystko jednak zależy od danego stanu faktycznego. Natomiast z perspektywy wykorzystywania technologii, warto tu wskazać, że już samo bezprawne przetwarzanie danych przez podmiot do tego nieuprawniony będzie rodziło ogromne ryzyko do pociągnięcia do odpowiedzialności. Zgodnie z Rozporządzeniem, na gruncie przepisów karnych, przetwarzanie danych osobowych, które jest niedopuszczalne albo dokonane przez osobę, która nie jest uprawniona do podejmowania takich czynności, jest zagrożone karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch. W przypadku, w którym czyn dotyczy danych osobowych o szczególnym znaczeniu (np. danych biometrycznych, danych ujawniających pochodzenie rasowe lub etniczne, danych dotyczących zdrowia), wymiar kary pozbawienia wolności został zwiększony do lat trzech. Przestępstwem w rozumieniu prawa karnego jest również udaremnianie lub utrudnianie przeprowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych. Czyn ten jest zagrożony karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch [9].

Szkoda jest jednym z kryteriów odpowiedzialności odszkodowawczej, a co za tym idzie, aby móc domagać się odszkodowania należy nie tylko ją wykazać, ale należy wykazać inne przesłanki odpowiedzialności. Jednocześnie warto w tym miejscu wskazać, zgodnie z tezą Sądu Apelacyjnego w Gdańsku, że przesłanką odpowiedzialności nie jest sama wina, ale szereg okoliczności, których łączne spełnienie może stanowić podstawę przyjęcia tej odpowiedzialności. Chodzi w szczególności, po pierwsze, o zdarzenie, z którym ustawa wiąże obowiązek naprawienia szkody, następnie powstanie szkody i po trzecie, istnienie związku przyczynowego między tym zdarzeniem a szkodą, jak już było wskazane wcześniej. Jednak dopiero w następnej kolejności, w razie stwierdzenia istnienia związku przyczynowego między konkretnym zdarzeniem a szkodą, (np. wyciekiem danych z konkretnego salonu kosmetycznego a użyciem tych danych w przestępstwie), będzie trzeba rozważać, jaka podstawa odpowiedzialności wchodzi w rachubę w danej sytuacji, tzn. czy mamy do czynienia z odpowiedzialnością na zasadzie winy, czy na zasadzie ryzyka, czy wreszcie na trzeciej podstawie tzw. zasady słuszności [11, 14].

Najważniejsze zatem jest to, aby szkoda była wykazana. Nie jest to łatwe, ale też nie jest to niemożliwe do realizacji. Szczególnie, że zgodnie z przepisami Rozporządzenia każdy administrator danych w chwili kiedy dojdzie do wycieku danych jest zobowiązany poinformować UODO o incydencie oraz co ważne, poinformować o tym fakcie osoby, których dane wyciekły. W sytuacji wycieku danych, ciężar udowodnienia spełnienia wszelkich kwestii bezpieczeństwa i ochrony danych będzie spoczywał na właścicielu salonu (zakładając, że jest administratorem danych), a udowodnienie szkody spoczywać będzie na kliencie (osobie, której dane wyciekły).

Na wykazanie szkody składa się szeroki zakres informacji, dokumentów, dowodów czyli wszystko to, co może potwierdzić zajście szkody. Jeżeli dane zostały wykorzystane do wzięcia pożyczki, będzie trzeba wykazać wszelką dokumentację z tym związaną, w tym również zawiadomienie złożone w tej sprawie na policji.

Jeżeli zatem doszło do wycieku danych, wówczas zdarzeniem będzie wyciek danych, szkodą będzie wzięcie pożyczki, natomiast najistotniejszą kwestią, którą należy wykazać to związek przyczynowo-skutkowy pomiędzy zdarzeniem a szkodą. Może jednak zdarzyć się tak, że klient próbując uzyskać odszkodowanie będzie konfabulował, bo w rzeczywistości np. sam zaciągnął zobowiązania w banku.

Katarzyna Kryla-Cudna wskazuje, że *„(...) okoliczność, że dany uszczerbek powstał nie wbrew woli uprawnionego, lecz za jego sprawą lub wolą nie eliminuje szkody"*. Kwestia ta może być istotna przy ustaleniu odpowiedzialności odszkodowawczej. Czyli przyczynienie się klienta do powstania szkody istotnie może wpłynąć na zakres odpowiedzialności podmiotu, który prowadzi salon beauty [18-20].

Udowodnienie faktu, że dany wyciek doprowadził do sytuacji, że ktoś użył danych klientki do zaciągnięcia pożyczki nie jest proste. Owszem istnieje takie prawdopodobieństwo, jednak jednoznacznie nie można wykluczyć sytuacji, w której klientka swoje dane podała dobrowolnie wypełniając dostępny formularz w internecie. Rozwiązanie tej problematyki będzie możliwe dopiero na etapie weryfikacji przez policję lub sąd.

ODPOWIEDZIALNOŚĆ ADMINISTRATORA DANYCH W SALONIE BEAUTY

W tej części warto zatrzymać się i wyjaśnić kim jest administrator, a kim jest osoba przetwarzająca. Otóż do administratora należy ustalenie celów na podstawie których dane osobowe będą przetwarzane. Administratorem zatem będzie podmiot odpowiedzialny i decydujący o tym po co i w jaki sposób mają być przetwarzane dane. Natomiast podmiotem przetwarzającym jest podmiot (np. zewnętrzny) wykonujący zadania dla danego salonu beauty. Może to być księgowa, firma wykonująca działania outsourcingowe, podmiot wykonujący obowiązki kadrowe, promocyjne itd. Za najczęstszy przykład przytacza się firmy informatyczne, które dostarczają oprogramowanie i zarządzają nim lub udostępniają przechowywanie danych w chmurze.

Istotę odpowiedzialności administratora danych w salonie beauty w świetle Rozporządzenia, opisuje artykuł 82, ust. 2. Wskazuje on na odpowiedzialność podmiotu przetwarzającego – *„Odpowiada on wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom"*. Jednocześnie należy zwrócić uwagę na zdanie pierwsze, które wskazuje, że każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze Rozporządzenie, a co za tym idzie należy rozróżnić dwie role: administratora i pomiotu przetwarzającego. Pełnią oni kluczowe role w zakresie przetwarzania danych, i w ich obowiązkach jest dopełnienie wszelkich czynności zmierzających do ochrony danych osobowych. Administrator i podmiot przetwarzający powinni w ramach podwyższonej należytej staranności zrobić wszystko co w ich mocy, aby dane osobowe były odpowiednio chronione [1].

Ustawodawca w ustępie 3 wskazał na przesłankę egzoneracyjną, czyli wyłączającą odpowiedzialność, a dokładniej – *„Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody"*. Zatem każdy z tych podmiotów może zwolnić się z odpowiedzialności jeżeli udowodni, że do wycieku nie doszło z jego winy. Tu dochodzimy do istotnego zagadnienia jakim jest wina.

Z treści ustępu drugiego dowiadujemy się, że każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze Rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze Rozporządzenie nakłada bezpośrednio na podmioty przetwarzające lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. W tym miejscu warto wskazać, że mamy do czynienia z odwróconym ciężarem dowodu. Jest to niezwykle ważne, albowiem co do zasady przyjmuje się zgodnie z artykułem 6 Kodeksu cywilnego, że *„ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne"*, a więc w normalnej sprawie (innej niż ochrona danych), gdzie klientka zostaje poszkodowana, to na niej spoczywa ciężar udowodnienia faktu, że doznała uszczerbku w danym salonie kosmetycznym. Jednak z perspektywy ochrony danych osobowych, to na przedsiębiorcy czyli osobie prowadzącej biznes w branży beauty będzie ciążył ciężar udowodnienia, że dopełnił wszelkich obowiązków wynikających z Rozporządzenia (RODO). Niewątpliwie zmienia to sytuację procesową pozwanego przedsiębiorcy [1, 11].

Z ustępu trzeciego dowiadujemy się o przesłankach egzoneracyjnych, czyli wyłączajacych odpowiedzialność. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. A więc, pomijając już fakt konieczności udowodnienia dołożenia podwyższonej należytej staranności przy wprowadzeniu i realizowaniu obowiązków wynikających z Rozporządzenia, to z tego ustępu dowiadujemy się, że przesłanką zwalniającą jest

udowodnienie, przez dany podmiot, że nie ponosi winy za np. wyciek danych. Choć należy podkreślić, że udowodnienie braku winy nie jest łatwe [1].

Ustęp czwarty wskazuje na sytuację, do której może dojść jeżeli występuje więcej podmiotów przetwarzających dane niż sam administrator czy przetwarzający. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. Odpowiedzialność solidarna, która jest tu wskazana dotyczy sytuacji, w której każda ze stron będzie odpowiadała w częściach równych do wysokości odszkodowania jakie przyzna sąd [1].

Z ustępu piątego i szóstego wynika, że administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2 omawianego artykułu. Natomiast ustęp szósty wskazuje na postępowanie sądowe dotyczące odszkodowania, a które jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2. Rozporządzenia [1].

PODSUMOWANIE

Zebranie powyższych rozważań pozwala zobrazować pewną należytą staranność jaką w minimalnym stopniu powinien spełnić każdy przedsiębiorca w kontekście ochrony danych osobowych, aby zminimalizować ryzyko odpowiedzialności odszkodowawczej. Najistotniejszymi są m.in obligatoryjne kwestie dokładnego przestrzegania Rozporządzenia (RODO), unikanie korzystania z aplikacji/oprogramowania, jeżeli nie można sprecyzować gdzie dane są udostępniane przez podmiot dostarczający daną aplikację. Jeżeli w przedsiębiorstwie dane gromadzone są w chmurze internetowej należy zweryfikować czy jest ona publiczna, czy prywatna oraz odpowiednio dostosować przepisy i zasady gromadzenia danych w firmie, aby spełniały wymogi prawne Rozporządzenia w tym zakresie.

Odpowiednie zabezpieczenie danych, przechowywanie w zamkniętych miejscach, należyte zabezpieczanie hasłem nośników danych, niewykorzystywanie komputerów, na których gromadzone są dane klientów do celów prywatnych, minimalizują ryzyko potencjalnego zarażenia go złośliwym oprogramowaniem. Świadomość i szacowanie ryzyka to pierwsze kroki do zgodności prawnej salonu beauty. Jeżeli jednak dojdzie do wycieku, najistotniejsze jest zminimalizowanie jego skutków. Dlatego konieczne jest przygotowanie procedury postępowania na wypadek wycieku danych, aby w sytuacji awaryjnej nie podejmować decyzji pod wpływem emocji tylko zgodnie z założeniami. Warto korzystać ze wsparcia prawników, aby pomogli odpowiednio przygotować salon do zgodności prawnej (*compliance*).

LITERATURA

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.
2. Dyrektywa 2009/24/WE. Programy komputerowe - ochrona prawna.
3. Włodek J. Wynalazki wykorzystujące programy komputerowe. Rzecznik Patentowy 2002, vol. 2(33): 40.
4. Sztobryn K. Ochrona programów komputerowych w prawie własności intelektualnej w Unii Europejskiej: 71.
5. Deloitte, Ochrona danych osobowych, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/ochrona-danych-osobowych.html (dostęp: 26.04.2020).
6. Wyrok Trybunału Sprawiedliwości z dnia 29 lipca 2019 r. C-40/17, Operator witryny internetowej jako administrator danych osobowych.
7. Przeprowadzenie anonimowej ankiety wśród przedsiębiorców na stronie www.kosmetykaprawo.pl, w dniu 12.08.2019 r., https://kosmetykaprawo.pl/podziel-sie-ze-mna-swoja-opinia-na-temat-aplikacji-mobilnych/ (dostęp: 26.04.2020).
8. Cloud computing RODO a lokalizacja serwerów poza Europejskim Obszarem Gospodarczym. Computerworld, https://www.computerworld.pl/news/Cloud-computing-RODO-a-lokalizacja-serwerow-poza-Europejskim-Obszarem-Gospodarczym,407576.html (dostęp: 26.04.2020).
9. Odpowiedzialność za naruszenie przepisów RODO. Poradnik przedsiębiorcy. https://poradnikprzedsiebiorcy.pl/-odpowiedzialnosc-za-naruszenie-przepisow-rodo (dostęp: 26.04.2020).
10. Zaniechanie w prawie karnym. Prokuratura w Zielonej Górze, http://www.zielona-gora.po.gov.pl/index.php?id=36&ida=3735 (dostęp: 26.04.2020).
11. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz.U.2019.1145 t.j. z dnia 19.06.2019 r.
12. Wyrok Sądu Apelacyjnego w Szczecinie z dnia 6 lipca 2018 r. I ACa 164/18.
13. Bierć A. Zarys Prawa Prywatnego. Wolters Kluwer Polska, Warszawa 2018: 295-403.
14. Bieniek G. (red.) Komentarz do Kodeksu cywilnego, Księga Trzecia Zobowiązania, tom 1 wydanie 7, Warszawa 2007: 240-554.
15. Scottish hairdressing company suffers data breach https://www.retailsecure.co.uk/blog/scottish-hairdressing-company-suffers-data-breach (dostęp: 26.04.2020).
16. Słownik języka polskiego, https://sjp.pwn.pl/slowniki/szkoda.html (dostęp: 26.04.2020).
17. Wyrok Sądu Apelacyjnego w Białymstoku. I ACa 724/16.
18. Rezler J. Naprawienie szkody wynikłej ze spowodowania uszczerbku na ciele lub zdrowiu (według Prawa cywilnego), RPEiS 1968: 21-22.
19. Jastrzębski J. Kara umowna, Warszawa. 2006: 111.
20. Kryla-Cudna K. Instytucje Prawa Cywilnego, Zadośćuczynienie pieniężne za szkodę niemajątkową powstałą wskutek niewykonania lub nienależytego wykonania umowy, Warszawa 2018: 3-4.
21. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, Dz.U.2019.1950 t.j. z dnia 14.10.2019.
22. Wyrok Sądu Apelacyjnego w Gdańsku z dnia 3 grudnia 2015 r. I ACa 600/15.
23. Wyrok Sądu Apelacyjnego w Łodzi z dnia 16 lipca 2019 r. III APa 12/19.
24. Wyrok Sądu Apelacyjnego w Gdańsku z dnia 31 maja 2016 r. V ACa 877/15.
25. Rodzaje chmur obliczeniowych http://cloudinfos.pl/Rodzaje-chmur-obliczeniowych (dostęp: 26.04.2020).

CITE / SPOSÓB CYTOWANIA
Lendzion C. Wpływ rozwoju technologicznego na odpowiedzialność odszkodowawczą. Aesth Cosmetol Med. 2020;9(3):329-336.