Paweł MALINOWSKI
Akademia Nauk Stosowanych w Nowym Sączu, Polska
ORCID: 0009-0006-3262-1356

ROLA I POTENCJAŁ SPOŁECZEŃSTWA W KONTROLI PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH

Streszczenie

Artykuł obejmuje swoim zakresem badanie aktualnie obowiązujących przepisów prawa w zakresie ochrony danych osobowych, dotyczących wybranych uprawnień osób fizycznych, których dane podlegają procesom przetwarzania przez administratorów danych. Uprawnienia te można potraktować jako swoiste narzędzia przekazane przez regulatora osobom fizycznym w celu sprawowania realnej kontroli nad przetwarzaniem ich danych osobowych u podmiotów dokonujących tych czynności. W pierwszej kolejności przeanalizowano prawo dostępu przysługujące osobie, której dane dotyczą, następnie prawo do usunięcia danych, czyli tzw. prawo do bycia zapomnianym, kolejno uprawnienie do ograniczenia przetwarzania danych osobowych podmiotu danych. Każdy ze zweryfikowanych przepisów nadawał kompetencje do zbadania, czy administrator w zakresie czynności wykonywanych na danych osobowych zastosował się do zasad płynących z rozporządzenia ogólnego o ochronie danych osobowych (RODO). Wynikiem przeprowadzonej analizy jest stwierdzenie, że stałe poszerzanie świadomości społecznej w zakresie bezpieczeństwa danych osobowych, czego skutkiem jest korzystanie z uprawnień regulacyjnych w zakresie sprawowania kontroli nad administratorami, pozwoli na osiągnięcie równowagi pomiędzy wykorzystaniem potencjału danych osobowych a ochroną prywatności osób fizycznych.

Słowa kluczowe: ochrona danych osobowych, rozporządzenie RODO, prawa osób fizycznych.

THE ROLE AND POTENTIAL OF THE PUBLIC IN CONTROLLING THE PROCESSING OF PERSONAL DATA

Summary

The article covers with its scope the examination of currently binding legal regulations in the area of personal data protection concerning selected entitlements of natural persons whose data are subject to processing by data controllers. These rights can be treated as specific tools provided by the regulator to the individuals in order to exercise real control over the processing of their personal data at the entities carrying out these activities. First of all, the right of access of the data subject was analysed, then the right to erasure of data, i.e. the so-called right to be forgotten, followed by the right to limit the processing of personal data of the data subject. Each of the reviewed provisions gave the competence to examine whether the controller, within the scope of activities performed on personal data, complied with the principles flowing from the General Data Protection Regulation (RODO). The result of the analysis is that the continuous expansion of public awareness of personal data security, resulting in the exercise of regulatory powers to control controllers, will achieve a balance between exploiting the potential of personal data and protecting the privacy of individuals.

Key words: data protection, RODO Regulation, rights of individuals.

Wprowadzenie

Dnia 25 maja 2018 roku weszło w życie Rozporządzenie Parlamentu Europejskiego i Radu UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych), co zmieniło dotychczasowe podejście do przetwarzania danych osobowych. Zmiany te miały na celu harmonizację prawa w ramach Unii Europejskiej i bardziej szczegółowe uregulowanie swobodnego przepływu danych osobowych. W ramach polskiego systemu prawnego wdrożenie RODO doprowadziło do nowelizacji aż 162 aktów prawnych. Efektem tych zmian było też zwiększenie poziomu prywatności osób fizycznych podczas wszelkich procesów, w ramach których dochodziło do czynności przetwarzania danych. Procesy przetwarzania danych miały być tak projektowane, by posiadały przymiot transparentności, a podmiot, którego dane są przetwarzane, powinien zostać skutecznie poinformowany o fakcie przetwarzania.

Każda osoba fizyczna, której dane podlegają przetwarzaniu, posiada szereg uprawnień względem podmiotu przetwarzającego. Jak pokazuje praktyka, świadomość społeczna w tym zakresie stale rośnie, niemniej często wiedza jednostki ograniczona jest wyłącznie do faktu, że administrator lub procesor posiadają obowiązek stosowania przepisów dotyczących ochrony danych osobowych. Czasami „szary obywatel" niekoniecznie wie, jakie konkretnie posiada w ramach tych przepisów uprawnienia względem przetwarzania na każdym jego etapie. Co za tym idzie, nadal dane osobowe wykorzystywane przez szereg podmiotów mogą być przetwarzane z naruszeniem przepisów, a osoby fizyczne, które leżą u podstaw tego procesu, nie wiedzą, z jakich narzędzi skorzystać i jak chronić się przed tymi naruszeniami.

W dzisiejszych czasach informacje stanowią jeden z najistotniejszych i najbardziej strategicznych zasobów każdej organizacji. W przypadku firm świadczących usługi lub obsługujących bezpośrednio osoby fizyczne bazy danych z klientami bądź potencjalnymi klientami stanowią informację kluczową dla prowadzenia efektywnego biznesu. Tym samym mogą pojawić się pokusy dotyczące zbierania znacznych ilości danych osobowych lub pozyskiwania ich ze źródeł nielegalnych. W takich przypadkach osoby fizyczne mogą niejako na własną rękę zweryfikować zasadność posiadania przez określony podmiot ich danych osobowych, a w efekcie dojść do przekonania, że dane te zostały pozyskane w nieodpowiedni sposób, tj. przetwarzane niezgodnie z przepisami prawa.

Celem niniejszej pracy jest przeprowadzenie analizy aktualnie obowiązujących przepisów prawa w zakresie ochrony danych osobowych, związanych z prawami osób, których dane są poddawane procesom przetwarzania. Badanie ukierunkowane jest na weryfikację możliwości sprawowania kontroli nad procesami przetwarzania danych osobowych u administratorów oraz potencjalnych skutków monitorowania podmiotów przetwarzających dla systemu ochrony danych osobowych w Polsce. Mając na względzie powszechność przetwarzania danych, zaprezentowano też konkretne sposoby i metody prowadzenia społecznej kontroli w zakresie zgodności przetwarzania z obowiązującymi regulacjami i procedury, które będą musiały zostać wdrożone po stronie administratora, odpowiadającego na wnioski osoby fizycznej korzystającej z uprawnień wynikających z przepisów prawa.

1. Podstawowe pojęcia w zakresie ochrony danych osobowych z perspektywy osób fizycznych

Analizując przepisy dotyczące ochrony danych osobowych, należy wyjść od samej definicji danych osobowych, które:

> oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej […]; 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 (Rozporządzenie Parlamentu Europejskiego i Rady 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 uchylenie dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), art. 4 pkt. 1).

Z przytoczonej definicji można wyciągnąć wniosek, że każda informacja, niezależnie od ilości danych, jakie przenosi, może stanowić dane osobowe, jeżeli na ich podstawie występuje możliwość identyfikacji konkretnej osoby fizycznej. Identyfikacja ta może mieć charakter zarówno bezpośredni, czyli wynikający wprost z posiadanych informacji na temat tej osoby, ale może też przyjąć formę pośrednią, tj. z wykorzystaniem dostępnych środków, np. narzędzi internetowych. Przykładem takich instrumentów mogą być ogólnodostępne portale społecznościowe, na których znajduje się znaczna ilość danych osobowych przypisanych do konkretnej osoby fizycznej. Wskazana możliwość połączenia danych osobowych przetwarzanych przez administratora z informacjami dotyczącymi osoby, zamieszczonymi w ramach mediów społecznościowych, jest właśnie sposobem na pośrednią identyfikację jednostki. Najlepszym przykładem, obrazującym, w jaki sposób przedstawiona powyżej wykładania przepisów może odnieść się do codziennego funkcjonowania osób fizycznych, będzie przyjrzenie się działalności firm telemarketingowych, które dzwonią do osób fizycznych, proponując różne usługi czy produkty. Nie wchodząc w dalsze rozmyślania w kwestii przekazywania informacji handlowych i rygorów wyrażenia oraz zbierania stosownych pozwoleń na takowe przekazywanie informacji, zastanówmy się nad tematem posiadania i przetwarzania danych osobowych przez wskazane firmy. Bardzo często w ramach kontaktów z tego typu organizacjami podmiot danych wnioskujący o wskazanie podstawy prawnej, która upoważnia firmę do kontaktu z osobą fizyczną, może otrzymać stosunkowo zwodniczą informację. Praktyka takich firm ukierunkowana jest na przekazanie podmiotowi danych komunikatu, jakoby jego numer został wygenerowany automatycznie, a z racji braku identyfikowalności, nie stanowi tym samym danych osobowych, więc administrator podczas kontaktu z losowo wygenerowanym numerem, nie jest w posiadaniu danych osobowych osoby fizycznej. Działalności firm telemarketingowych posługujących się opisaną procedurą kontaktu z osobami fizycznymi stoi zatem na pograniczu prawa. Niemniej jednak Autor skłaniałby się do oceny, że w ramach takich ścieżek kontaktu mamy do czynienia z nielegalnym przetwarzaniem danych osobowych osób fizycznych,

gdyż wskazane organizacje działają na dużych bazach danych i można z całą dozą pewności domniemywać, że część tych wygenerowanych numerów telefonów jest realnie weryfikowalna i możliwa do powiązania z konkretną osobą, a co za tym idzie – osoba ta jest identyfikowalna. W tym miejscu należy dodatkowo zwrócić uwagę, że często można spotkać się z twierdzeniem, że dane osobowe to wyłącznie informacje, takie jak numer pesel, numer telefonu, adres e-mail itd. Naturalnie są to informacje, na podstawie których można zidentyfikować konkretną osobę, ale należy również pamiętać, że mogą być to też inne dane, które na gruncie przepisów RODO będzie się uznawać za dane osobowe. Przykładem takich informacji mogą być np. preferencje zakupowe konkretnych podmiotów, przetwarzane przez sklepy internetowe. Często portale badają zakupy swoich klientów w celu przedstawienia im najbardziej dopasowanej reklamy i te preferencje połączone z pozostałymi informacjami posiadanymi przez sprzedawcę będą stanowiły dane osobowe. W działalności wielu przedsiębiorców, którzy obsługują osoby fizyczne, będą pojawiały się informacje o podmiotach danych, które w połączeniu z innymi informacjami (nawet takimi, które mogą zostać pozyskane pośrednio) stanowić będą dane osobowe, a co za tym idzie – będą podlegać ochronie na podstawie przepisów rozporządzenia RODO. Kolejnym takim przykładem będzie deweloper sprzedający nieruchomość, wchodzący w posiadanie wiedzy w temacie mocy nabywczej konkretnej osoby procesującej zakup np. mieszkania. Informacja, że ten konkretny podmiot danych posiada zdolność kredytową lub dysponuje środkami pozwalającymi na zakup nieruchomości będzie stanowić daną osobową dla tego przedsiębiorcy. Reasumując, należy pamiętać, że szereg informacji, które posiadają o nas administratorzy, mogą być danymi osobowymi, a każda osoba, której dane dotyczą, powinna być świadoma, że te informacje będą podlegać formalnej ochronie prawnej.

Rozważając dalej kwestię dotyczącą istotnych z punktu widzenia osób fizycznych definicji, które zostały zawarte w rozporządzeniu RODO, należy wyjaśnić termin „przetwarzanie danych osobowych". Z konkretnym objaśnieniem przychodzi słownik definicji, zawarty w rozporządzeniu opisujący przetwarzanie danych osobowych, jako:

> operacje 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 (Ibidem, art. 4 pkt 2).

Jak widać w przytoczonym przepisie, regulator wskazał możliwie jak najwięcej czynności, które stanowią przetwarzanie, ale niezależnie od przytoczonych przykładów lista ta nie stanowi katalogu zamkniętego i wszelkie inne czynności, w ramach których będą wykorzystywane dane osobowe, wyczerpywać będą znamiona przetwarzania. Z punktu widzenia osób, których dane podlegają przetwarzaniu, jest to bardzo istotna definicja, gdyż realnie pokazuje, w jakich sytuacjach i podczas wykonywania jakich działań administrator ma obowiązek stosowania przepisów z zakresu ochrony danych osobowych. Mając wiedzę na temat faktu, czym są dane osobowe i jakie czynności

wyczerpują definicje przetwarzania danych osobowych, można mieć podstawy do rozważań w temacie zasadności, celowości, legalności itd. działań wykonywanych przez administratorów. U podstawy każdej analizy dotyczącej przetwarzania danych osobowych leży weryfikacja, czy mamy do czynienia z informacjami o osobie, które spełniają przesłanki pozwalające uznać wskazaną informację za dane osobowe. W kolejnym etapie należy zweryfikować, czy czynność wykonywana z wykorzystaniem tych informacji nosi znamiona przetwarzania. Należy przyjąć, że jeśli na podstawie analizy stwierdzimy, że zbiór informacji stanowi dane osobowe, to wszystkie czynności, jakie będą wykonywane z wykorzystaniem tych informacji, będą ich przetwarzaniem.

Wciąż występujący szum informacyjny wokół RODO nastawia społeczeństwo na traktowanie regulacji jako całkowicie zbędnej oraz generującej tylko dodatkowe obostrzenia oraz wymogi, które w efekcie nie przynoszą spodziewanych rezultatów, a wyłącznie dają możliwość nakładania dotkliwych kar finansowych przez organ nadzorczy, jakim jest Urząd Ochrony Danych Osobowych. Niestety na takim przekazie korzystają wyłącznie organizacje wykorzystujące dane z naruszeniem przepisów dotyczących ochrony danych osobowych.

W tym miejscu należy również objaśnić definicję naruszenia ochrony danych osobowych, które zgodnie z treścią rozporządzenia: „oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" (Ibidem, art. 4 pkt. 12). Wyjaśnienie, jakie dostarcza regulator, nie jest w pełni przejrzyste i oczywiste dla osób, których dane są przetwarzane, czym bowiem realnie jest naruszenie bezpieczeństwa. Należy się też zastanowić, czy obywatel nieposiadający specjalistycznej wiedzy, będzie w stanie zweryfikować, czy doszło do naruszenia w zakresie przetwarzania jego danych osobowych, a tym samym – czy jest uprawniony do wysnuwania żądań względem administratora lub czy posiada podstawę dokonania zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych. W pewnych okolicznościach kwestia stwierdzenia naruszenia będzie prosta, np. w sytuacji, gdy podmiot danych otrzyma informację od organizacji, z którą dotychczas nie współpracował i nie wyrażał stosownych zgód na przetwarzanie. Natomiast często zaistnienie naruszenia wcale nie będzie oczywiste do stwierdzenia, a wręcz nie będzie możliwe bez weryfikacji dokumentacji posiadanej przez administratora i tym samym bez wykorzystania prawa dostępu do danych osobowych (które zostanie wyjaśnione w dalszej części opracowania). Rozważmy przykład, w którym osoba fizyczna współpracuje z organizacją w ramach świadczenia usługi A na jej rzecz. W pewnym momencie osoba ta otrzymuje komunikat dotyczący usługi B, świadczonej przez tego samego administratora. W takim stanie faktycznym, żeby stwierdzić, czy doszło do incydentu bezpieczeństwa danych, należy zweryfikować posiadaną przez administratora dokumentację w zakresie udzielonych pozwoleń, np. marketingowych, i tak, jeśli podmiot danych udzielił zgody na przekazywanie informacji handlowych dotyczących usług administratora, to najprawdopodobniej nie będzie w tym przypadku mowy o naruszeniu. Jeśli jednak administrator nie pozyskał odpowiednich pozwoleń od osoby fizycznej i dokonał przetwarzania jej danych w innym celu niż pierwotnie zostały zebrane, tj. kontaktu ukierunkowanego na przedstawienie oferty innej usługi, to w takim przypadku będziemy mieć do czynienia z naruszeniem. Reasumując, z punktu

widzenia osób, których dane podlegają procesom przetwarzania, trudne może być stwierdzenie, kiedy administrator przetwarza dane niezgodnie z przepisami. W takich sytuacjach z pomocą przychodzi urząd ochrony danych osobowych, który na swojej stronie internetowej publikuje formularz zgłoszenia skargi. Zgłoszenie jest całkowicie bezpłatne i w takim przypadku to urząd przejmie na siebie weryfikację, czy doszło do naruszenia przepisów i w efekcie posiada uprawnienie do nałożenia kar (Dmochowska, Zadrożny, 2018, s. 182), w tym też sankcji finansowych, na organizację niewłaściwie przetwarzającą dane osobowe.

2. Jakie prawa chroni RODO

Wczytując się pobieżnie w tytuł rozporządzenia RODO, można dojść do wniosku, że jest to akt prawny dotykający kwestii bezpieczeństwa danych osobowych osób fizycznych. Takie postrzeganie sprawy może powodować wytworzenie skrótu myślowego, że RODO to wyłącznie zbiór regulacji dotyczących ochrony danych osobowych, a nic bardziej mylnego. Zapoznając się z art. 1 pkt 2 rozporządzenia, należy podkreślić, że dokument ten ma na celu ochronę podstawowych praw i wolności osób fizycznych ze szczególnym uwzględnieniem prawa do ochrony danych osobowych. Zaznajomienie się z treścią tego przepisu daje możliwość spojrzenia na tematykę ochrony danych osobowych w zdecydowanie szerszym kontekście. Dokonując analizy wskazanego artykułu, należy zauważyć, że zamiarem rozporządzenia jest ochrona podstawowych praw i wolności osób fizycznych, a w szczególności ich praw do ochrony danych osobowych. Jak zatem należy zdefiniować podstawowe prawa i wolności osób fizycznych? Tutaj z pomocą przychodzi inny dokument opracowany i stosowany w ramach państw członkowskich Unii Europejskiej, tj. Karta Praw Podstawowych (Karta Praw Podstawowych Unii Europejskiej z dnia 14 grudnia 2007 r.). Zgodnie z informacją dostępną na stronie Rzecznika Praw Obywatelskich: „Karta praw podstawowych jest jednym z najważniejszych narzędzi ochrony praw podstawowych na poziomie regionalnym, jaki kiedykolwiek stworzono. Definiuje wartości, które nie podlegają negocjacjom" (https://bip.brpo.gov.pl/pl/content/karta-praw-podstawowych-i-jej-znaczenie-dla-polskiego-systemu-prawnego, dostęp: 25.04.2019). Karta to dokument podpisany w dniu 7 grudnia 2000 r. w Nicei, a później z pewnymi poprawkami dnia 12 grudnia 2007 r. w Lizbonie, który zawiera zbiór fundamentalnych praw człowieka i obowiązków obywatelskich. Artykuł 8 Karty Praw Podstawowych dotyczy ochrony danych osobowych. Wynika z niego, że każdy ma prawo do ochrony swoich danych, a ich przetwarzanie ma być rzetelne i prowadzone wyłącznie w określonych celach. Artykuł ten porusza również kwestie sprawowania kontroli nad tym obszarem, wskazując, że czynności kontrolne wykonuje niezależny organ. Wracając do przytoczonych na początku praw i wolności osób fizycznych, które ma chronić RODO, nie można zamknąć się wyłącznie na wskazany art. 8 Karty, lecz na tę tematykę należy spojrzeć z szerzej perspektywy. W ocenie Autora, RODO dotyka też innych praw i wolności wskazanych w Karcie Praw Podstawowych, np. prawa do wolności oraz bezpieczeństwa osobistego, o którym stanowi art. 6. Analizując temat uprawnienia do wolności, należy też brać pod uwagę wolność w zakresie przetwarzania danych osobowych i tutaj RODO dostarcza rozwiązania dla podmiotów danych, które dają swobodę w zakresie przetwarzania ich danych osobowych, gdyż np. możemy dokonać wyboru podmiotu przetwarzającego, zdecydować, jakie dane zostaną przekazane, kiedy proces przetwarzania zostanie zakończony. Odniesienie przepisów RODO do

bezpieczeństwa osobistego powinno być intuicyjne, gdyż regulacje dostarczane przez rozporządzenie mają na celu tworzenie systemu, który w sposób bezpieczny przetwarza dane osobowe, które są dobrem przypisanym do konkretnej jednostki (Wróbel, 2019, s. 201-225).

Niemniej jednak w ramach niektórych procesów przetwarzania administrator wchodzi w posiadanie danych dotyczących kwestii prywatności osoby, jak również może posiadać wiedzę np. w zakresie informacji o rodzinie podmiotu danych. Łatwo można sobie to wyobrazić na przykładzie pracodawcy, którego pracownik zgłasza członka rodziny do objęcia go ubezpieczeniem zdrowotnym w ramach zgłoszenia do Zakładu Ubezpieczeń Społecznych. Efektem takiej, oczywistej i spotykanej na co dzień, czynności będzie powzięcie wskazanych danych przez pracodawcę i tutaj RODO traktuje jasno, że informacje te są danymi osobowymi, co za tym idzie – administrator musi powziąć odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa tych informacji (Kępa, 2019, s. 22-23). Powyższy przykład również znajduje swoje odwzorowanie w art. 7 Karty Praw Podstawowych, który mówi o poszanowaniu życia prywatnego i rodzinnego. Jest to kolejny dowód na to, że rozporządzenie chroni wiele praw jednostki, ale przez pryzmaty bezpieczeństwa danych osobowych. Często słyszy się o tzw. danych wrażliwych, które zostały zdefiniowane w poprzedniej regulacji prawnej dotyczącej ochrony danych osobowych, tj. w ustawie z 1997 roku o ochronie danych osobowych w ramach art. 27 pkt. 1 tej ustawy (Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych). Na kanwie aktualnie obowiązujących przepisów dane wrażliwe zostały określone jako dane szczególnych kategorii i opisane w art. 9 RODO, m.in. zostały tam wskazane informacje dotyczące przekonań religijnych, poglądów politycznych czy kwestii światopoglądowych. W sytuacji, gdy tego rodzaju dane są przetwarzane, administrator musi spełnić dodatkowe wymagania stawiane przez regulatora. Tym samym treść rozporządzenia wpisuje się w art. 10 Karty Praw Podstawowych, który traktuje o wolności myśli, sumienia i religii.

Powyższe odwołania do unijnej regulacji, wskazującej fundamentalne prawa i wolności człowieka, to jedynie przykłady, gdyż w rozporządzeniu o ochronie danych osobowych znajduje się jeszcze wiele odnośników do innych praw podstawowych opisanych w Karcie, co pokazuje szeroki zakres wpływu niniejszego aktu na codzienne bezpieczeństwo życia osób fizycznych. RODO dotyka więc bardzo rozległego spektrum oddziaływania na zabezpieczanie podstawowych praw oraz wolności osób fizycznych, narzucając na administratorów przymus takiego sterowania procesami biznesowymi, aby na każdym etapie ich stosowania nie dochodziło do naruszeń tych uprawnień.

3. Wybrane uprawnienia osób fizycznych w stosunku do administratorów przetwarzających ich dane osobowe

Mając na względzie powyżej przytoczone przepisy i wskazane informacje, należy zauważyć, że rozporządzenie RODO stanowi akt prawny w sposób znaczący chroniący prywatności człowieka. Dowodem na prawdziwość przytoczonej tezy są wskazane i wyczerpująco opisane prawa osób, których dane podlegają procesom przetwarzania. Prawa te zostały wymienione w artykułach od 15 do 23 RODO, co już na samym wstępie pokazuje, że regulator w sposób bardzo szczegółowy podchodzi do uprawnień osób fizycznych względem administratorów, choćby ze względu na ilość oraz obszerność

poświęconych tej tematyce przepisów. Takie działanie jednoznacznie wskazuje, że prawodawcy zależy na maksymalizacji ochrony prywatności jednostki i przekazuje na jej ręce narzędzia pozwalające na weryfikację podmiotów przetwarzających i sposobów przetwarzania danych osobowych. Niemniej jednak w tym kontekście należy też mieć na względzie, że administrator nie zawsze będzie musiał spełnić żądania podmiotu danych, które zostały opisane w przepisach. Takie uprawnienie organizacji przetwarzającej dane osobowe pozwala na ochronę jej interesów w ramach wykonywanej działalności gospodarczej i utrzymanie ciągłości funkcjonowania. Potraktowanie regulacji w ten sposób też jest zasadne i niezbędne, gdyż w innym przypadku mogłaby wystąpić poważna dysproporcja między interesami osób fizycznych, których dane są przetwarzane, a administratorami, którzy tych przetwarzań dokonują (Fajgielski, 2019, s. 100-102). Należy jednak podkreślić, że w ocenie Autora, RODO przechyla szalę praw i wolności w kierunku osób fizycznych względem podmiotów przetwarzających.

Przechodząc do analizy wybranych uprawnień podmiotów danych, wypada wspomnieć o niestety nadal pojawiających się naruszeniach ochrony danych osobowych, a konkretnie o wciąż występujących zdarzeniach dotyczących handlu danymi osobowymi, gdzie nabywca wykorzystuje na własne potrzeby pozyskane od zbywcy informacje o osobach. W takim przypadku mamy do czynienia z sytuacją, w której podmiot danych będzie zastanawiał się, na jakiej podstawie nieznany administrator wchodzi z nim w interakcję, skąd nieznany administrator posiada dane osobowe umożliwiające wejście we wspomnianą interakcję, a także czy przetwarzanie zgodne jest z celem, jaki był wskazany w pierwotnym procesie, na bazie którego pozyskane zostały dane osobowe przez przedsiębiorcę. Przykładem tutaj może być otrzymanie informacji handlowej od organizacji, z którą dana osoba fizyczna nigdy nie współpracowała. W ramach takiego stanu faktycznego podmiot danych posiada uprawnienia do ustalenia formalnych podstaw przetwarzania, a w kolejnym kroku, w myśl art. 15 RODO, będzie mógł żądać dostępu do danych posiadanych przez konkretnego administratora. Zgodnie z oceną P. Fajgielskiego, w komentarzu do RODO (2022, s. 254-263), wskazany przepis gwarantuje prawo do uzyskania informacji, czy dane osobowe tej osoby są przetwarzane w ramach organizacji, a w sytuacji uzyskania odpowiedzi pozytywnej uprawnia wnioskodawcę do dostępu do danych na jej temat i uzyskania informacji o okolicznościach przetwarzania. Zatem na podstawie wskazanego przepisu podmiot ma prawo otrzymać informację w temacie celu przetwarzania. Jest to jeden z najbardziej kluczowych elementów wskazanego przepisu ze względu na fakt, że każda czynność przetwarzania danych osobowych musi odbywać się w konkretnym i sprecyzowanym celu, a u podwalin tego celu musi być wskazana jedna z podstaw prawnych wymienionych w art. 6 ust. 1 RODO, gdzie regulator wskazał przypadki, w których przetwarzanie jest zgodne z prawem (Mielniczek, 2021, s. 16). W sytuacji, gdy administrator nie potrafi wskazać właściwej podstawy prawnej przetwarzania, mamy do czynienia z działaniem niezgodnym z przepisami prawa, a czynność, w której wykorzystywane są dane osobowe wnioskodawcy jest nielegalna. Natomiast w ramach prawa dostępu do danych podmiot posiada jeszcze szereg innych uprawnień względem administratora, m.in. prawo do otrzymania wyczerpującej informacji w temacie odbiorców lub kategorii odbiorców, które mogą wejść w posiadanie danych tego podmiotu. Takie zapytanie daje szansę na prześledzenie drogi danych osobowych osób fizycznych i w rezultacie powzięcie informacji w temacie liczby podmiotów czy organizacji, które będą przetwarzać otrzymane informacje, a tym samym skutkuje

możliwością sprawowania kontroli nad procesem przetwarzania danych osobowych powierzonych jednej organizacji. Pozwala również na ocenę, czy nie dochodzi do ewentualnych naruszeń. Co ciekawe, osoba, której dane dotyczą, zgodnie z przytoczonym przepisem, ma też prawo żądać od administratora wydania kopii danych osobowych podlegających przetwarzaniu. Administrator, jeśli tylko takie przekazanie nie naruszy interesów osób trzecich, ma obowiązek udostępnić kopię danych, o które zwróci się podmiot przetwarzający. Dodać należy, że przekazywana kopia musi być udostępniona w odpowiednim i możliwym do odczytania formacie. Realnie, realizacja wskazanego uprawnienia podmiotu danych przez administratora możne nastręczać nie lada trudności, szczególnie w sytuacji dużych organizacji, które do przetwarzania danych wykorzystują znaczną ilość systemów informatycznych, a w proces przetwarzania zaangażowanych jest dużo osób oraz działów firmy. Tym bardziej, jeżeli przedsiębiorca jest rozproszony terytorialnie. Jak zatem w takiej sytuacji może wyglądać proces realizacji wniosku osoby fizycznej wnoszącej o wydanie kopii danych? Naturalnie należy mieć na względzie, że RODO nie definiuje kwestii proceduralnych, dając administratorowi pełną dowolność w zakresie sposobu działania ukierunkowanego na realizację wniosku. Najpewniej podmiot danych takie roszczenie skieruje na dedykowany adres mailowy, który posiada komórka zajmująca się ochroną danych osobowych we wskazanej organizacji. Po zapoznaniu się z prośbą będzie musiała zostać dokonana weryfikacja danych wnioskodawcy, ponieważ podmiot przetwarzający zobowiązany jest do potwierdzenia tożsamości wnioskującego, a może się to wydarzyć przy pomocy zadania kilku pytań pomocniczych na bazie już posiadanych informacji o osobie. Kolejno jednostki odpowiedzialne za poszczególne czynności przetwarzania będą zobowiązane do sprawdzenia wszystkich systemów i ewentualnych lokalizacji danych osobowych wnioskodawcy, czyli będą musiały zweryfikować wszystkie zasoby, w ramach których wykonywane są procesy przetwarzania. W dużych organizacjach często zlokalizowanie wszystkich danych wiąże się z potrzebą zaangażowania do procesu wielu osób, co w sposób znaczący wydłuża realizację takich wniosków. Z pomocą przychodzi tutaj regulator, który wskazuje narzędzie, jakim jest rejestr czynności przetwarzania opisany w art. 30 ust. 1 RODO, który powinien w sposób kompleksowy wskazać wszystkie działania podejmowane w zakresie przetwarzania danych osobowych. Dobrą praktyką w tym zakresie jest tworzenie rejestru szerszego niż minimum opisane we wskazanym przepisie i dodanie również informacji dotyczącej lokalizacji zasobów danych w strukturze organizacyjnej i informatycznej (Jagielski, 2022, s. 205). Wracając do meritum rozmyślania, po zlokalizowaniu wszystkich żądanych informacji, będzie trzeba je przygotować, może też wyeksportować do odpowiednich formatów, z którymi podmiot danych będzie się w stanie swobodnie zapoznać. Etapem wieńczącym całą procedurę będzie realizacja wniosku podmiotu i przesłanie kopii danych. Podsumowując, art. 15 RODO narzuca na administratorów tworzenie procesów biznesowych, w ramach których przetwarzane są dane osobowe w taki sposób, aby istniała możliwość weryfikacji i udostępnienia danych osobowych osoby fizycznej na każdym etapie wykonywanych czynności i w ramach wszystkich posiadanych zasobów informatycznych (Litwiński, 2021, s. 249-251).

Kolejnym, ważnym z perspektywy osób fizycznych, uprawnieniem zawartym w RODO jest tzw. „prawo do bycia zapomnianym", opisane w art. 17, czyli prawo do usunięcia danych osobowych. Przepis ten ma na celu umożliwienie żądania od administratora usunięcia danych dotyczących wnioskodawcy w sytuacji wystąpienia

przynajmniej jednej ze wskazanych przesłanek, m.in. podmiot danych wycofał zgodę na przetwarzanie, dane podmiotu nie są już niezbędne do realizacji celów, w ramach których zostały zebrane, dane osobowe były przetwarzane niezgodnie z prawem. Zgodnie z komentarzem do RODO (Czerniawski, 2018, s. 522-530), mamy tutaj do czynienia z dwoma uprawnieniami podmiotu danych, tj. do żądania usunięcia danych (regulowanym przez art. 17 ust. 1) i do żądania do bycia zapomnianym (regulowanym przez art. 17 ust. 2), które to uprawnienie uzależnione jest od kwestii lokalizacji przetwarzania przez administratora danych osobowych. W sytuacji, kiedy administrator upublicznił dane osobowe, podmiot danych posiada uprawnienia do bycia zapomnianym, a tym samym administrator musi usunąć wszystkie dane osobowe, w których posiadaniu się znajduje i poinformować o tym jeszcze pozostałych administratorów, którzy również dane te przetwarzają. Natomiast zgodnie z art. 17 ust. 1, administrator zobowiązany jest do usunięcia danych w ramach swoich zasobów. Niezależnie od powyższej analizy należy zauważyć, że często skutki realizacji wniosku osoby fizycznej znacząco odbiegają od zamierzeń, jakie najprawdopodobniej posiadał regulator, tworząc wskazany przepis. Sytuację tę łatwo obrazuje prosty przykład dotyczący realizacji umowy kupna: sprzedaży między sklepem a osobą fizyczną. Naturalnie w takim przypadku mówimy o przetwarzaniu danych osobowych w związku z realizacją usługi. Po zakończeniu obsługi klienta oraz dostarczeniu zamówionego produktu klient posiada uprawnienie do złożenia wniosku dotyczącego całkowitego usunięcia jego danych osobowych. Jak w takiej sytuacji zachowa się rozsądny przedsiębiorca? Oczywiście, zgodnie z procedurą, zobowiązany jest najpierw zweryfikować tożsamość wnioskodawcy, a pomijając pozostałe kroki formalne, w takim stanie faktycznym klient najprawdopodobniej otrzyma informację, że administrator jedynie usuwa dane osobowe, które były niezbędne do procesu zamówienia i realizacji zamówienia. Administrator, dbając o swój prawnie uzasadniony interes, który został opisany w art. 6 ust. 1 lit. f RODO i który może stanowić podstawę prawną przetwarzania (Dmochowska, Zadrożny, 2018, s. 22), zachowa dane osobowe klienta niezbędne do obsługi ewentualnego roszczenia ze strony tegoż klienta. Takie dane administrator będzie przechowywał do czasu upływu ustawowego terminu dochodzenia roszczeń, a po tym czasie zostaną one usunięte, zgodnie z zasadą minimalizacji przetwarzanych danych osobowych. Reasumując, realnym efektem wykorzystania uprawnienia do bycia zapomnianym będzie prawdopodobnie częściowe pozbawienie administratora pewnych informacji o osobie wnioskodawcy. Niemniej jednak, mimo ułomności tego uprawnienia, daje ono możliwość podmiotowi danych odcięcia się od organizacji, która przetwarza dane z naruszeniem przepisów i tutaj przykładem jest Wyrok Naczelnego Sądu Administracyjnego z dnia 30 listopada 2021 r., który wprost stwierdził, że w sytuacji, gdy dane osobowe są przetwarzane niezgodnie z prawem osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych. Innym przykładem, gdzie prawo do usunięcia danych okaże się bardzo przydatne dla osób fizycznych będzie sytuacja, w której, w związku z upływem czasu, administrator usunie część informacji o kliencie, mając na względzie zasadę minimalizacji danych, np. okres możliwości zgłoszenia ewentualnych roszczeń upłynął. Natomiast administrator nadal będzie przetwarzał dane w związku z pierwotnie udzielonymi zgodami, np. marketingowymi, a także w związku z założonym kontem zakupowym na portalu sklepu. Tutaj wykorzystanie prawa do usunięcia danych powinno spowodować całkowite odcięcie się od organizacji w ramach każdej czynności, w której przetwarzane

były dane osobowe wnioskodawcy. W zależności od konkretnego stanu faktycznego, osoba powołująca się na prawo do bycia zapomnianym może zatem uzyskać efekt intuicyjnie zamierzony, czyli usunięcia dotyczących jej danych osobowych. W ocenie Autora, ułomność tego przepisu i procesu jest duża ze względu na fakt, że w wielu przypadkach realnie dane osobowe podmiotu danych będą wciąż przetwarzane przez administratora w związku z innymi celami przetwarzania.

Opisując uprawnienia osób fizycznych w ramach przetwarzania ich danych, wypada nadmienić, że w ramach wszystkich gwarancji, jakie daje RODO, jest jeszcze kwestia dotycząca ograniczenia przetwarzania danych osobowych, opisana w art. 18. Według Autora, jest to bardzo istotne uprawnienie, gdyż pozwala na zatrzymanie wszystkich procesów przetwarzania, jakie występują u danego administratora, a tym samym daje pewność, że ten nie może w żaden dostępny sposób manipulować posiadanymi danymi. Wojewódzki Sąd Administracyjny w wyroku z dnia 15 listopada 2019 r. stwierdzi, że skutkiem skorzystania przez podmiot danych z uprawnienia do ograniczenia przetwarzania ma być sprowadzenie procesów przetwarzania posiadanych przez administratora danych wyłącznie do ich przechowywania. Naturalnie, tak jak w przypadku prawa do bycia zapomnianym, tak tutaj, regulator wskazuje konkretne sytuacje, w których osoba fizyczna może żądać ograniczenia przetwarzania. Należy pamiętać, że katalog tych sytuacji jest bardzo szeroki i daje możliwość złożenia wniosku choćby w związku z podejrzeniem, że jakieś przetwarzane dane są nieprawidłowe. Co za tym idzie, wystarczy jedynie podejrzenie, aby móc skorzystać z uprawnienia. Należy w tym miejscu podkreślić, że w sytuacji uprawdopodobnienia ewentualnego naruszenia po stronie administratora danych, osoba której dane dotyczą, może rozpocząć weryfikację procesów przetwarzania, jakim podlegają jej dane osobowe, właśnie od sprecyzowania żądania w przedmiocie ograniczenia przetwarzania. Takie działanie automatycznie pozwoli na utrzymanie *status quo* sprawy i dokładne zbadanie zasadności domysłów w zakresie ewentualnego naruszenia.

Podsumowując, każda osoba, której dane są przetwarzane, posiada szereg praw wskazanych i szczegółowo opisanych w rozporządzeniu dotyczącym ochrony danych osobowych. Ponadto może realnie ingerować w proces przetwarzania na każdym etapie tego procesu, dokonując weryfikacji, czy administrator działa w zgodzie z przepisami prawa. Niemniej jednak na tym nie kończą się regulacje opisane w RODO, dotyczące uprawnień podmiotów danych, ponieważ w art. 12 rozporządzenia znajdują się zasady, w jaki sposób administrator ma obowiązek przekazywać informacje, komunikować się oraz w jakim trybie ma wykonywać prawa osoby, której dane dotyczą. Ustęp pierwszy przywołanego artykułu wskazuje, że administrator ma obowiązek komunikować się z osobą w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (Kołodziej, 2020, s. 97). Ponadto informacje muszą być udzielane w formie, jakiej żąda podmiot danych, np. ustnie. Niestety z perspektywy zasady rozliczalności (Lubasz, Szkurłat, 2023, s. 70-71), która również jest sprecyzowana w przepisach rozporządzenia i dotyczy możliwości przedstawienia materiału dowodowego na poczet ewentualnej kontroli wykonywanej przez organ nadzoru, ciężko będzie udowodnić, że wniosek podmiotu danych został wykonany właściwie podczas rozmowy, ale w tym przypadku jest to zmartwienie administratora. Idąc dalej, ustęp drugi tego artykułu informuje, że administrator zobowiązany jest ułatwić osobie, której dane dotyczą, wykonanie jej praw m in. również tych opisanych wcześniej. W motywie 59 preambuły

RODO wyjaśniono, że m.in. pomoc ta ma się objawić jako bezpłatne wykonywanie czynności ukierunkowanych na realizację praw osób, których dane dotyczą. Zdecydowanie należy podkreślić, że administrator nie ma podstawy do odmowy podjęcia działań związanych z realizacją praw osoby fizycznej, chyba że nie jest jej w stanie zidentyfikować. Dodatkowo, przepis art. 12 wskazuje, że administrator realizuje wnioski podmiotu danych bez zbędnej zwłoki, a w każdym razie nie później niż w terminie miesiąca od otrzymania żądania. Jeśli podmiot przetwarzający nie zrealizuje praw wnioskodawcy w tym czasie, zmuszony jest poinformować w terminie miesiąca od momentu otrzymania żądania o powodach niepodjęcia działań i o możliwości wniesienia skargi do organu nadzorczego (Bielak-Joma, Lubasz, 2018, s. 464-476).

Powyżej przywołane przepisy dotyczące sposobu realizacji wniosków osób fizycznych pokazują, jak duży wpływ na procesy przetwarzania danych przez konkretnego administratora może mieć osoba, której dane podlegają przetwarzaniu i jak szerokie są uprawnienia do wpływania na czynności przetwarzania wykonywane przez administratora. W ocenie Autora, zarówno ilościowy, jak również jakościowy zakres uprawnień, jakimi dysponują osoby fizyczne względem przetwarzania, daje możliwość dużej ingerencji w weryfikację procesów biznesowych, w ramach których przetwarzane są dane osobowe. Realizacja praw podmiotów danych po stronie administratora często może okazać się bardzo pracochłonna i wymagająca zaangażowania dużej ilości zasobów osobowych oraz informatycznych.

Podsumowując, realizacja praw osób fizycznych, których dane są przetwarzane, może nastręczać administratorowi dużo pracy i trudności. Niemniej jednak RODO, narzucając przymus dbania o prywatność osób fizycznych, wymaga od administratorów działania w ramach pełnej zgodności z przepisami. Wszystkie te trudności mają na celu zabezpieczenie danych osobowych osób fizycznych i ochronę ich praw oraz wolności, mając na względzie ryzyko potencjalnych naruszeń. Aby działać w zgodzie z treścią rozporządzenia, administrator musi już na samym początku, podczas projektowania czynności operacyjnych, w ramach wykonywanej działalności gospodarczej, mieć na względzie ochronę danych osobowych i tak planować swoje procesy, aby na każdym ich etapie był w stanie zrealizować uprawnienia podmiotów danych. Zdaniem Autora, jedynie poprzez ciągłe powiększanie świadomości społecznej w tematyce ochrony danych osobowych można mieć nadzieję na rzetelne stosowanie przepisów w różnego rodzaju organizacjach. Dziś nadal można spotkać się z podmiotami, które funkcjonują, jakby rozporządzenie nie dotyczyło ich działalności, ponadto organ nadzoru nie jest w stanie skontrolować ogromnej rzeszy przedsiębiorców działających w Polsce. W sytuacji, gdy każda z osób, której dane podlegają przetwarzaniu, będzie świadoma swych praw i będzie z nich korzystać, to niejako samoistnie wymusi na przedsiębiorcach przymus funkcjonowania zgodnie z RODO. Realnie to właśnie oddziaływanie podmiotów danych na administratorów, a w efekcie obligatoryjność realizacji wniosków tych podmiotów i obawa przed zgłoszeniem do organu nadzorującego, a w konsekwencji nałożenie wysokich kar finansowych, spowoduje takie opracowanie czynności, w ramach których administratorzy przetwarzają dane, aby istniała możliwość realizacji praw osób fizycznych.

Podsumowanie

Wraz z rozwojem technologii i coraz większą ilością danych gromadzonych przez różne organizacje, podstawowe prawa jednostki, jaką w tym przypadku jest osoba fizyczna, są narażane na stale rosnącą liczbę ewentualnych naruszeń. W ramach powyżej przytoczonych aspektów z zakresu prawa ochrony danych osobowych, należy wysnuć wniosek, że regulator unijny, uaktualniając przepisy o ochronie danych osobowych rozporządzeniem RODO, wpłynął na poprawę bezpieczeństwa i prywatności osób fizycznych w ramach procesów przetwarzania danych osobowych. Dodatkowo podmioty, których dane dotyczą, posiadają szereg narzędzi prawnych, pozwalających na przeprowadzenie weryfikacji czynności przetwarzania u administratorów, ale także dających możliwość wpłynięcia na sposób i zakres tego przetwarzania. Opisane uprawnienia jednostki w stosunku do firm czy instytucji mają również znaczenie dla ogółu społeczeństwa, gdyż wpływają na obniżenie ryzyka ewentualnych naruszeń lub bezpośrednio wystąpienia potencjalnych przestępstw, a tym samym pozwalają na zachowanie większej swobody przy udostępnianiu danych osobowych. Dzieje się tak w związku z faktem, że regulacja ta skutkuje narzuceniem na administratorów szeregu obowiązków w zakresie ochrony prywatności osób fizycznych, których celem jest zabezpieczenie podstawowych praw obywateli.

Świadomość społeczna w zakresie ochrony danych osobowych stale wzrasta, co pokazuje badanie przeprowadzone przez Urząd Ochrony Danych Osobowych w maju 2022 roku (https://uodo.gov.pl/pl/file/4104, dostęp: 12.07.2023) pt. „Wiedza na temat bezpieczeństwa danych osobowych w Polsce". Na bazie danych statystycznych raport ten wskazuje, że coraz więcej Polaków wie, w jaki sposób zadbać o bezpieczeństwo swoich danych osobowych, a wiedza ta występuje szczególnie u osób młodych, w wieku 18-34 lata. Niestety, mimo swoich przekonań, to właśnie w tej grupie dochodzi najczęściej do popełniania błędów, jakim jest np. udostępnianie haseł osobom trzecim czy też pozostawianie swoich danych w ankietach internetowych. Niemniej jednak należy zauważyć, że od momentu wejścia w życie rozporządzenia o ochronie danych osobowych zarówno świadomość, jak i wiedza osób fizycznych w zakresie bezpieczeństwa ich prywatności znacząco wzrosła. Niestety, pomimo ciągłego rozwoju oszuści, którzy stanowią zagrożenie dla bezpieczeństwa danych, stale znajdują nowe możliwości i sposoby na wyłudzanie danych osobowych, a w efekcie do ich wykorzystywania na niekorzyść ich właścicieli. Reasumując, poprzez skuteczne podnoszenie świadomości społecznej i odpowiedzialne zarządzanie danymi przez instytucje publiczne, sektor przedsiębiorców prywatnych oraz inne organizacje, będziemy w stanie zbliżyć się do osiągnięcia równowagi pomiędzy wykorzystaniem potencjału danych osobowych a ochroną prywatności osób fizycznych.

Bibliografia

Bielak-Jomaa, E., Lubasz, D. (red.). (2018). *RODO ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Warszawa: Wydawnictwo Wolters Kluwer.

Dmochowska, A., Zadrożny, M. (2018). *Unijna reforma ochrony danych osobowych*. Warszawa: C.H. Beck.

Fajgielski, P. (2019). *Prawo ochrony danych osobowych*. Warszawa: Wydawnictwo Wolters Kluwer.

Fajgielski, P. (2022). *Komentarz do rozporządzenia nr 2016/679 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) Komentarz*. Warszawa: Wydawnictwo Wolters Kluwer.

Jagielski, M. (2022). *Dokumentacja Ochrony Danych Osobowych ze Wzorami*. Warszawa: Wydawnictwo Wolters Kluwer.

Karta Praw Podstawowych Parlamentu Europejskiego, Rady i Komisji Europejskiej z dnia 14.12.2007 r. (Dz.U.UE.C.2007.303.1).

Kępa, L. (2018). *Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców.* Warszawa: Wydawnictwo C.H. Beck.

Kępa, L. (2019). *Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku*. Warszawa: Wydawnictwo C.H. Beck.

Kołodzieja, M. (2020). *Vademecum Inspektora Ochrony Danych Osobowych*. Warszawa: Wydawnictwo C.H. Beck.

Kowalski, M. (2020). *Poradnik dla początkującego inspektora ochrony danych*. Warszawa: Wydawnictwo Wiedza i Praktyka sp. z o. o.

Litwiński, P. (red.). (2021). *Ogólne Rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Lubasz, D. (red.). (2019). *Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wydawnictwo Wolters Kluwer.

Lubasz, D., Szkurłat, A. (red.). (2023). *Ochrona danych osobowych. Poradnik praktyczny*. Warszawa: Wydawnictwo Wolters Kluwer.

Mielniczek, P. (2021). *Ochrona danych osobowych od A do Z w 16 krokach*. Warszawa: Wydawnictwo C.H. Beck.

Rozporządzenie Parlamentu Europejskiego i Rady 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.U. UE. L. 2016.119.1).

Rzecznik Praw Obywatelskich. (2023). Karta Praw Podstawowych i jej znaczenie dla polskiego systemu prawnego. Pobrane z: https://bip.brpo.gov.pl/pl/content/karta-praw-podstawowych-i-jej-znaczenie-dla-polskiego-systemu-prawnego.

Sieradzka, A., Wieczorek, M. (2020). *Monitoring zgodny z RODO, Praktyczny poradnik z wzorami dla sektora publicznego i prywatnego*. Warszawa: Wydawnictwo C.H. Beck.

Urząd Ochrony Danych Osobowych. (2022). *Wiedza na temat bezpieczeństwa danych osobowych w Polsce, Raport z badania maj 2022*. Pobrane z: https://uodo.gov.pl/pl/file/4104.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., Nr 1781, poz. 1781).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r., Nr 133, poz. 883).

Wróbel, A. (red.). (2019). *Karta Praw Podstawowych Unii Europejskiej. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Wyrok Naczelnego Sądu Administracyjnego z 30 listopada 2021 r., sygn. akt III OSK 4558/21 (LEX nr 3264199).

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 15 listopada 2019 r., sygn. akt II SA/Wa 1504/19 (LEX nr 3041492).