LEGALNOŚĆ POZYSKIWANIA I PRZETWARZANIA DANYCH OSOBOWYCH W SFERZE PUBLICZNEJ

Aspekty praktyczne

Mariusz Jabłoński, Krzysztof Wygoda

Wolters Kluwer

LEGALNOŚĆ POZYSKIWANIA I PRZETWARZANIA DANYCH OSOBOWYCH W SFERZE PUBLICZNEJ

Aspekty praktyczne

Mariusz Jabłoński, Krzysztof Wygoda

Wolters Kluwer

WARSZAWA 2021

SPIS TREŚCI

WPROWADZENIE

Ponad trzy lata od daty rozpoczęcia bezpośredniego stosowania postanowień rozporządzenia Parlamentu Europejskiego i Rady (UE) 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[1] (dalej: rozporządzenie ogólne; RODO) racjonalne wydaje się kontynuowanie merytorycznych badań, które poświęcone są wybranym zagadnieniom dotyczącym interpretacji jego przepisów, ze szczególnym uwzględnieniem kwestii legalności pozyskiwania i przetwarzania danych przez administratorów sfery publicznej[2] oraz zasad ochrony dokumentów i informacji z nimi związanych, a znajdujących się w ich posiadaniu. Jeśli uwzględnić aktywność krajowego organu ochrony (Prezesa Urzędu Ochrony Danych Osobowych) i sądów administracyjnych, formułowanie ocen dotychczasowej praktyki wy-

[1] RODO uchyla i zastępuje dyrektywę 95/46/WE w obszarze sektorów prywatnego i publicznego w państwach członkowskich. Konieczne staje się jednocześnie podkreślenie, że obok RODO przyjęta została dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (tzw. dyrektywa policyjna), Dz.Urz. UE L 119, s. 89.

[2] Z zasady skutku bezpośredniego prawa unijnego wynika możliwość powoływania się przez jednostki i inne uprawnione podmioty bezpośrednio na normę prawa unijnego (tu: RODO) względem swojego państwa (będącego państwem członkowskim UE). Jednocześnie trzeba podkreślić, że błędne jest identyfikowanie daty wejścia w życie RODO z dniem 25.05.2018 r. Od tej daty postanowienia rozporządzenia ogólnego mają zastosowanie – art. 99 ust. 2 RODO.

wiązywania się przez administratorów z ciążących na nich obowiązków dokumentacyjnych zdefiniowanych w RODO i innych regulacjach krajowych wydaje się w pełni uzasadnione.

Legalność pozyskiwania i przetwarzania danych ma dla oceny prawidłowości działań podejmowanych przez administratora fundamentalne znaczenie. Konieczne jest przede wszystkim wskazanie na kompleksowość i wzajemnie przenikanie się zasad odnoszących się do tego obszaru regulacji. Widoczne jest to choćby w potrzebie łącznej interpretacji przesłanek legalizujących procesy przetwarzania i traktowania art. 9 ust. 2 RODO jako niezbędnego uzupełnienia przesłanek wskazanych w art. 6 RODO.

Kolejną kwestią wymagającą pogłębienia było (i w dalszym ciągu jest) nadużywanie przez administratora dyrektywy odnoszącej się do stosowania zgody jako przesłanki legalizującej proces przetwarzania. Podstawa ta ma bowiem pierwszeństwo, ale tylko w sytuacji braku innych przesłanek legalizujących. Wielu administratorów ze sfery publicznej nie pamięta o takim kontekście jej stosowania i zdecydowanie jej nadużywa, nie bacząc przy tym na generowane w ten sposób zagrożenia dla prowadzonych przez siebie procesów przetwarzania.

Warto też pamiętać, że nawet prawidłowe umocowanie procesu przetwarzania nie przesądza o legalności przetwarzania jako takiego, gdyż administrator, zaniedbując realizację części obowiązków ustanowionych w art. 5 RODO, najprawdopodobniej doprowadzi do naruszenia prawa, i to nawet w przypadku braku incydentów skutkujących pojawieniem się naruszenia ochrony danych osobowych. Przykładem tego typu uchybienia zasadom przetwarzania jest choćby niezapewnienie właściwej rozliczalności prowadzonych procesów (np. wskutek braków w dokumentacji ochrony).

Jeżeli z bezpośrednim stosowaniem postanowień RODO wiąże się konieczność systemowej zmiany podejścia do ochrony danych osobowych w aspekcie materialnym, to automatycznie muszą też zmienić się metody dokumentowania przez administratorów tych wszystkich czynności, które podejmowane są zarówno w odniesieniu do zorganizowania, jak

i zapewnienia stałej funkcjonalności systemu ochrony przetwarzania danych. Zarówno administrator, jak i podmiot przetwarzający mają obowiązek aktywnego zabiegania o ochronę prywatności na każdym etapie przetwarzania oraz na każdym etapie projektowania procesów przetwarzania – wskazuje na to reguła *Privacy by Design* oraz *Privacy by Default*.

Samo RODO, nie precyzując ścisłego wykazu dokumentacji czy jakichś poziomów bezpieczeństwa i procedur i nie zawierając w swej treści również konkretnych wytycznych organizacyjnych ani technologicznych dotyczących odpowiedniego zabezpieczenia przez administratora danych, definiuje jednak obowiązki na nim ciążące, których wykonanie powinno wiązać się z wytworzeniem odpowiednich dokumentów oraz posiadaniem niezbędnych do tego informacji.

Posiadane przez administratorów dokumenty, informacje, jak i same dane osobowe są coraz częściej przedmiotem żądań kierowanych na podstawie odrębnych uprawnień dostępowych gwarantowanych (konstytucyjnie i ustawowo) nie tylko obywatelom, ale także szerokiemu kręgowi uprawnionych. Jeśli uwzględnić ten fakt, jak również to, że samo RODO nie wyklucza legalności udostępnienia danych osobowych znajdujących się w posiadanych przez administratora dokumentach urzędowych, zasadne jest przeprowadzenie badań w tym zakresie.

W prezentowanej monografii staraliśmy się spojrzeć na wskazane wyżej kwestie w sposób uwzględniający specyfikę kształtującego się cały czas systemu ochrony danych osobowych. Nieuprawnionym uproszczeniem byłoby stwierdzenie, że już teraz wiemy wszystko to, co wynika z „życia regulacji" po dacie rozpoczęcia jej obowiązywania, a w omawianym przypadku – bezpośredniego stosowania. Proces ten będzie długotrwały, szczególnie jeżeli weźmiemy pod uwagę, że RODO i regulacje ustawowe posługują się wielością zwrotów niedookreślonych, często o autonomicznym charakterze, które dopiero po upływie określonego czasu „odnajdą" swoją treść w realiach naszego krajowego systemu źródeł prawa i ich stosowania.

Jednocześnie nie budzi naszej wątpliwości, że nowe otwarcie, które nastąpiło po 25.05.2018 r., nie może być uznane za prostą kontynuację dorobku wypracowanego w latach 1997–2018 tak na poziomie dorobku naukowego, jak i na poziomie orzecznictwa sądowego. Wbrew pozorom – naszym zdaniem – zmieniło się bardzo dużo, choć może nie do końca jest to jeszcze widoczne.

Prezentowana monografia ma na celu podjęcie próby analitycznego spojrzenia na dokonane przez ustawodawcę unijnego modyfikacje z jednoczesnym zweryfikowaniem tego, czy wpłynęło to na praktykę funkcjonowania administratorów, oczywiście przy uwzględnieniu wcześniej podejmowanych w tym kierunku badań.

Monografia ta jest czwartą z kolei, którą w okresie ostatnich pięciu lat udaje się nam zaprezentować. Wcześniejsze publikacje[3] poświęcone były istotnym zagadnieniom z zakresu ochrony danych, identyfikowanym z punktu widzenia oczekiwanego rozpoczęcia bezpośredniego stosowania RODO i działań podejmowanych przez polskiego ustawodawcę przed tą datą (pierwsze dwa opracowania), a także dostrzeganym już problemom praktycznym (publikacja z 2019 r.). W ramach prezentowanej publikacji staramy się kontynuować część wątków zainicjowanych w dotychczasowych opracowaniach, ze szczególnym uwzględnieniem tych, które nie zostały jeszcze poddane analizie, oraz z rozwinięciem zagadnień, które z perspektywy już ponad trzyletniej praktyki nadal okazują się być niezrozumiałe lub budzą wątpliwości administratorów, w szczególności ze sfery publicznej. Tak postawione zadanie prowadzi jednak – z uwagi na konieczność zapewnienia przejrzystości wywodu – do omawiania treści częściowo zbieżnych z poruszanymi we wcześniejszych publikacjach.

[3] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017; M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018; M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO. Wybrane zagadnienia*, Wrocław 2019.

Zakończenie niniejszego opracowania pierwotnie planowane było na drugą połowę 2020 r. Wirus, który stał się wyznacznikiem nowych wzorców życia i społecznej egzystencji, również na nas i naszych Bliskich odcisnął niestety swoje piętno, co spowodowało w konsekwencji wydłużenie prac. Dziękując Wydawnictwu, jak i zawsze życzliwym nam Pracownikom redakcji, a także wszystkim tym, którzy mentalnie nas wspierali, mamy nadzieję, że zaproponowane rozwiązania, jak również przedstawione kierunki interpretacji, okażą się trafne oraz pomocne z punktu widzenia tak praktyków, jak i wszystkich badaczy zagadnień związanych z ochroną danych osobowych.

Mariusz Jabłoński, Krzysztof Wygoda

Wrocław, kwiecień 2021 r.

Rozdział I

PRZESŁANKI POZYSKIWANIA DANYCH OSOBOWYCH PRZEZ PODMIOTY PUBLICZNE

1. Zagadnienia wstępne – konieczność i możliwość różnicowania zakresu pozyskiwania informacji przez władze publiczne

Fakt pozyskiwania danych osobowych w ramach działania podmiotów publicznych nie jest ani zaskakujący, ani kontrowersyjny. Oczywiste jest bowiem, że działając w ramach realizacji swoich zadań, muszą one dysponować wiedzą niezbędną do prawidłowego korzystania z przysługujących im kompetencji. Przy czym właśnie owa niezbędność informacji stanowi oś podziału pomiędzy legalnością pozyskiwania danych osobowych a działaniami wykraczającymi poza granice dopuszczalnego działania.

Należy przy tym podkreślić, że w modelu demokratycznego państwa prawa w centrum zainteresowania władzy publicznej leży zaspokajanie potrzeb jednostek. Ma ono jednak uwzględniać poszanowanie przysługujących im praw oraz ich możliwie dużą swobodę decyzyjną w zakresie wchodzenia w interakcje ze strukturami szeroko pojętego państwa. Społeczeństwa demokratyczne powinny bowiem szanować odrębność budujących je jednostek. Jednym z elementów systemowych

mających na celu zagwarantowanie poszanowania godności człowieka (będącej źródłem wszystkich wolności i praw człowieka) w wymiarze indywidualnego postrzegania członków społeczeństwa jest – chroniona od dłuższego już czasu – prywatność czy wręcz autonomia informacyjna jednostki[1].

W Polsce takie dychotomiczne postrzeganie tych dwu pokrewnych obszarów ochrony wolności i praw jednostki wynika choćby z gwarancji udzielonych w art. 47, 51 i art. 53 ust. 7 Konstytucji RP[2]. Jednak zarówno prywatność, jak i samookreślenie informacyjne (autonomia informacyjna) nie są chronione w sposób bezwzględny i podlegają choćby ograniczeniom spełniającym warunki określone w art. 31 ust. 3 Konstytucji RP[3]. Ogólnie rzecz ujmując, wprowadzenie ograniczeń praw czy nawet wolności nie budzi wątpliwości, jeżeli przemawia za tym inna norma, zasada lub wartość konstytucyjna, a stopień tego ograniczenia pozostaje w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to ma służyć. Jeśli zatem władze publiczne podejmują działania w kontekście przestrzegania klauzuli konieczności, w demokratycznym społeczeństwie wykazać muszą odpowiednio doniosłą potrzebę społeczną uzasadniającą wprowadzenie ograniczeń prywatności i samookreślenia

[1] Zob. szerzej: J. Braciak, *Prawo do prywatności*, Warszawa 2004, s. 161 i n.

[2] Szerzej na temat konstytucyjnego wymiaru ochrony prywatności i ochrony danych osobowych zob. np.: K. Wygoda, *Prawo do ochrony danych osobowych w Konstytucji RP* [w:] *Meritum. Ochrona danych osobowych,* red. D. Lubasz, Warszawa 2020, s. 45–57 i wskazane tam orzecznictwo oraz literatura. Na temat tzw. infosfery zob. T. Górzyńska, *Prawo do informacji i zasada jawności administracyjnej w orzecznictwie Sądu Najwyższego, Naczelnego Sądu Administracyjnego i Trybunału Konstytucyjnego*, Kraków 1999, s. 21. Z punktu widzenia traktowania praw jako wartości: R. Piotrowski, *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjn*e [w:] *Prywatność a jawność. Bilans 25-lecia i perspektywa na przyszłość*, red. A. Mednis, Warszawa 2016, s. 18–31.

[3] Warto też zauważyć, że Wielka Izba Europejskiego Trybunału Praw Człowieka 17.10.2019 r. wydała wyrok w sprawie López Ribalda i inni przeciwko Hiszpanii. Stwierdzono w nim, że stosowanie wobec pracowników ukrytego nadzoru za pomocą kamer wideo może być usprawiedliwione w określonych sytuacjach. Ma to miejsce w sytuacji, gdy zachodzi uzasadnione podejrzenie poważnych uchybień pracowniczych oraz ryzyko dużych strat firmy. Wówczas – jak podkreślił Europejski Trybunał Praw Człowieka – nie będziemy mieli do czynienia z naruszaniem praw do prywatności oraz do sprawiedliwego procesu. Oczywiście każdy przypadek musi być oceniany z perspektywy konkretnych okoliczności.

informacyjnego (autonomii informacyjnej) oraz ich proporcjonalność w stosunku do realizowanego celu, pamiętając jednocześnie, że wszelkie ograniczenia muszą być przewidziane w akcie o randze ustawy[4] (co zgodnie z art. 91 ust. 3 Konstytucji RP obejmuje również takie ograniczenia, które wynikać będą z rozporządzeń i dyrektyw unijnych)[5].

Uchwycenie odpowiednich proporcji pomiędzy wszystkimi istotnymi wartościami, tj.: potrzebą zapewnienia sprawności działania państwa, choćby w kontekście umożliwienia ochrony praw i wolności innych osób, zapewnieniem bezpieczeństwa państwa, porządku publicznego, konieczności ochrony środowiska bądź zdrowia publicznego jest kluczowe dla określenia zakresu niezbędności informacji znajdujących się w posiadaniu podmiotów publicznych.

Warto jednak pamiętać, że kwestia niezbędności w demokratycznym państwie nie może być utożsamiana wprost z zasadami celowości przetwarzania i jego minimalizacji wynikającymi z RODO czy DODO – które funkcjonują w nieco innym kontekście badania legalności procesów przetwarzania danych osobowych. Chcąc zatem wyprowadzać z Konstytucji zasady dające się pogodzić z regułami wynikającymi z tych dwu aktów unijnych, uwzględniające przy tym konstytucyjny

[4] W orzeczeniu K 28/98 Trybunał Konstytucyjny stwierdził, że konieczna szczegółowość („głębokość") regulacji ustawowej „zależy od normowanej materii – w niektórych dziedzinach (np. prawo karne, czy mówiąc szerzej – regulacje represyjne) zarysowuje się bezwzględna wyłączność ustawy, nakazująca normowanie w samej ustawie właściwie wszystkich elementów definiujących stronę podmiotową czy przedmiotową czynów karalnych" – wyrok z 9.11.1999 r., K 28/98 (OTK 1999/7, poz. 156). Mniej ukształtowany charakter ma natomiast orzecznictwo Trybunału w innych dziedzinach niż prawo karne i podatkowe. W innym ze swych rozstrzygnięć wskazał, że „w odniesieniu do sfery wolności i praw człowieka, zastrzeżenie wyłącznej ustawowej rangi unormowania ich ograniczeń należy pojmować dosłownie, z wykluczeniem możliwości [...] przekazania kompetencji normodawczej innemu organowi" – wyrok TK z 19.05.1998 r., U 5/97, OTK 1998/4, poz. 46.

[5] Na temat zasady pierwszeństwa z perspektywy ustawodawcy unijnego zob.: D. Kornobis-Romanowska, *Rozporządzenie o ochronie danych osobowych – charakter prawny, zakres stosowania i skutek w prawie krajowym państw członkowskich* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017, s. 27 i n.

zakaz dyskryminacji i obowiązek równego traktowania, należy przyjąć szerokie ujęcie podmiotu chronionego w art. 47 i 51 Konstytucji RP (a zatem postrzeganie go jako osoby fizycznej poddanej władztwu RP, a nie wyłącznie jako obywatela RP).

Wszelkie podmioty publiczne, które chciałyby rozszerzać zakres gromadzonych informacji o osobach innych niż obywatele RP, pozostają bowiem związane wymogiem podejmowania działań niezbędnych w demokratycznym państwie. Prawo do ochrony informacji o sobie samym nie jest uprawnieniem o charakterze politycznym – uzasadnionym realizacją jakiegokolwiek przejawu suwerenności narodu, a tylko odnalezienie takiego powiązania pozwalałoby na różnicowanie traktowania obywateli i innych osób przebywających na terytorium RP. Zarówno ochrona prywatności, jak i ochrona danych osobowych przynależą do szerokiej grupy wolności i praw osobistych jednostki (nie tylko z uwagi na systematykę Konstytucji RP, ale także z uwagi na ich istotę), a zatem narodowość czy obywatelstwo nie stanowią *per se* istotnego składnika statusu prawnego osoby, która chce z nich korzystać. Jeżeli zatem podmioty publiczne, by realizować swoje zadania, mogą różnicować podejście do jednostki, dysponując jedynie jakąś przesłanką istotną z punktu widzenia celu podejmowanych działań, to trudno jest wskazać, jaki relewantny element statusu osoby niebędącej obywatelem RP uzasadniłby zbieranie przez władze jej danych w zakresie innym niż niezbędny w państwie demokratycznym. Zatem, tak jak w przypadku różnych celów i zadań uzasadniających zbieranie odmiennych zakresowo danych o obywatelach, również w przypadku osób niebędących obywatelami RP możliwość zbierania ich danych osobowych o innym zakresie niż dopuszczalny w odniesieniu do obywateli musi wynikać bezpośrednio z realizowanego celu lub zadania, a nie z faktu, że jednostka nie jest obywatelem RP.

Zauważyć trzeba, że posługując się wykładnią literalną, można uznać, że postanowienia Konstytucji RP (a w szczególności jej art. 51) adresowane są głównie do organów państwa (mowa jest przecież o władzach publicznych czy urzędowych dokumentach i zbiorach danych), nie można jednak na tej podstawie wnioskować, że pozostałe podmioty nie podlegają ograniczeniom narzuconym przez ten przepis. Podej-

ście takie jako nazbyt wąskie niezgodne byłoby również z założeniem horyzontalnego oddziaływania norm konstytucyjnych[6]. Jak słusznie zauważyła I. Lipowicz, będąca pomysłodawcą większości rozwiązań konstytucyjnych poświęconych ochronie informacji o charakterze osobowym, w tym oczywiście art. 51, nie ma w jego ust. 1 „podziału na sektor publiczny i prywatny. Oznacza to, że również żądanie informacji ze strony elektrowni czy telekomunikacji wymaga – jeżeli ma stać się obowiązkiem informacyjnym – podstawy ustawowej. Udzielenie informacji o sobie może być częścią umowy, musi jednak pozostawać w jej granicach i dawać swobodę wyboru"[7].

Uznanie horyzontalnego obowiązywania konstytucji we wszystkich obszarach, które mogą być nim objęte, i odejście od ściśle wertykalnych relacji państwo – obywatel jest niewątpliwie podstawą jej bezpośredniego stosowania i sprzyja budowaniu społeczeństwa otwartego, a w kontekście omawianych regulacji jest też gwarancją pozwalającą na tworzenie społeczeństwa informacyjnego[8]. Jak największa pewność zakresu przysługujących jednostkom praw jest bowiem elementem upodmiotawiania się społeczeństwa, które w ich obronie może sięgać bezpośrednio do aktu rangi najwyższej, nie czekając na działania legislacyjne ustawodawcy[9]. Podejście takie zapewnia zatem niezbędną pewność ochrony danych, zwłaszcza wtedy, gdy zadania państwa nie są wykonywane bezpośrednio przez jego organy, gdy dochodzi do tzw. prywatyzacji administracji czy

[6] Horyzontalne obowiązywanie wolności i praw jednostki związane jest zatem z dopuszczeniem możliwości powoływania się przez osoby fizyczne, a także osoby prawne, na gwarantowane konstytucyjnie uprawnienia w zakresie rozstrzygania sporów cywilnoprawnych i pracowniczych, do jakich może między nimi dochodzić. W takim ujęciu normy konstytucji mogłyby się stać podstawą rozstrzygania tych sporów.

[7] I. Lipowicz, *Konstytucyjne prawo do informacji a wolność informacji* [w:] *Wolność informacji i jej granice*, red. G. Szpor, Katowice 1997, s. 14.

[8] Zob. szerzej: M. Kuliński, *Regulacje komunikacji elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, Warszawa 2010, s. 4 i n.

[9] Inaczej oddziaływanie art. 51 widzi jednak M. Wild, który bazując na literalnym brzmieniu uprawnień sformułowanych np. w ust. 3 omawianej regulacji, uznaje, że „domaganie się od podmiotów niepublicznych uzyskania dostępu do danych na swój temat nie znajduje zatem podstawy w art. 51 ust. 3, lecz wymaga uzasadnienia na gruncie ogólnego prawa do ochrony życia prywatnego" – M. Wild [w:] *Konstytucja RP*, t. 1, *Komentarz art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, s. 1232.

Stan prawny na 15 czerwca 2021 r.

Recenzent
Dr hab. Agnieszka Grzelak, prof. ALK

Wydawca
Dagna Kordyasz

Redaktor prowadzący
Paulina Ambroży

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8246-272-2

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

Książka omawia legalne pozyskiwanie i przetwarzanie danych osobowych przez administratorów sfery publicznej oraz wskazuje najskuteczniejsze metody ochrony dokumentów i informacji zawierających takie dane.

Autorzy wyodrębnili obszary łączące ochronę danych osobowych (podstawy przetwarzania danych) z obowiązkami dokumentacyjnymi. Przedstawione zostały fundamentalne zasady dotyczące ochrony przedmiotowych dokumentów, także w kontekście realizacji przez uprawnionych ich praw dostępowych.

Publikacja jest przeznaczona zarówno dla pracowników administracji, zobowiązanych do stosowania omawianych przepisów, jak i wszystkich podmiotów będących administratorami danych osobowych.

Mariusz Jabłoński – profesor nauk prawnych, nauczyciel akademicki; kierownik Katedry Prawa Konstytucyjnego na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz kierownik studiów podyplomowych ochrony danych osobowych na tymże wydziale; autor licznych publikacji naukowych.

Krzysztof Wygoda – doktor nauk prawnych, adiunkt na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego; autor licznych publikacji naukowych.

9788382462722 W01P01

ISBN 978-83-8246-272-2

9 788382 462722

CENA 99 ZŁ (W TYM 5% VAT)