

OCHRONA DANYCH OSOBOWYCH W ŚCIGANIU PRZESTĘPSTW

Standardy krajowe i unijne

Martyna Kusak, Paweł Wiliński

OCHRONA DANYCH OSOBYCH W ŚCIGANIU PRZESTĘPSTW

Standardy krajowe i unijne

Martyna Kusak, Paweł Wiliński

Zamów książkę w księgarni internetowej

profinfo.pl
księgarnia internetowa

Publikacja dofinansowana z grantu Narodowego Centrum Nauki
Nr 2015/19/B/HS5/00122

Stan prawny na 1 lutego 2020 r.

Recenzent

Dr hab. Agnieszka Grzelak, prof. ALK

Wydawca

Monika Pawłowska

Redaktor prowadzący

Kinga Zajac

Opracowanie redakcyjne

Agata Czuj

Projekt okładek serii

Wojtek Kwiecień-Janikowski, Przemek Dębowski

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

prawolubni

SZANUJMY PRAWO I WŁASNOŚĆ
Więcej na www.legalnakultura.pl
POLSKA IZBA KSIĄŻKI

© Copyright by

Wolters Kluwer Polska Sp. z o.o., 2020

ISBN 978-83-8187-632-2

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. 22 535 82 19

e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów	9
Wstęp	13
Rozdział I	
Potrzeba ochrony danych osobowych w sprawach karnych	17
Rozdział II	
Zakres przedmiotowy przepisów o ochronie danych osobowych	23
2.1. Dyrektywa 2016/680.....	23
2.2. Ustawa krajowa	26
2.3. Wnioski	39
Rozdział III	
Standardy jakości ochrony danych osobowych	41
3.1. Standardy jakości ochrony danych osobowych jako kryterium.....	41
3.2. Standardy jakości danych osobowych	42
3.2.1. Prawidłowość (dokładność).....	42
3.2.1.1. Standard unijny	42
3.2.1.2. Standard krajowy	46
3.2.1.3. Wnioski.....	56
3.2.2. Adekwatność, stosowność i proporcjonalność	57
3.2.2.1. Standard unijny	57
3.2.2.2. Standard krajowy	60
3.2.2.3. Wnioski.....	65

3.3. Standardy jakości przetwarzania danych osobowych.....	66
3.3.1. Przetwarzanie zgodne z prawem i rzetelne	66
3.3.1.1. Standard unijny	66
3.3.1.2. Standard krajowy	69
3.3.1.3. Wnioski.....	72
3.3.2. Zbieranie danych w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzanie w sposób niezgodny z tymi celami	74
3.3.2.1. Standard unijny	74
3.3.2.2. Standard krajowy	78
3.3.2.3. Wnioski.....	80
3.3.3. Ograniczenie przechowywania danych	80
3.3.3.1. Standard unijny	80
3.3.3.2. Standard krajowy	81
3.3.3.3. Wnioski.....	82
3.3.4. Zasada bezpieczeństwa danych.....	83
3.3.4.1. Standard unijny	83
3.3.4.2. Standard krajowy	85
3.3.4.3. Wnioski.....	87

Rozdział IV

Ochrona danych osobowych w wybranych czynnościach

organów ścigania	89
4.1. Inwigilacja.....	89
4.1.1. Uproszczony dostęp do danych.....	89
4.1.2. Reakcja Strasburga i Luksemburga.....	94
4.1.2.1. Europejski Trybunał Praw Człowieka: inwigilacja, również masowa, dopuszczalna pod pewnymi warunkami ...	94
4.1.2.2. Trybunał Sprawiedliwości Unii Europejskiej: wysoki standard ochrony.....	99
4.1.3. Inwigilacja a dane osobowe	108
4.1.4. Prawo krajowe.....	116
4.1.5. Wnioski.....	124
4.2. Automatyczne podejmowanie decyzji i profilowanie.....	127
4.2.1. Znaczenie automatycznego podejmowania decyzji...	127
4.2.2. Dopuszczalność i warunki stosowania	131

4.2.3. Transparentność	135
4.2.4. Prawo krajowe	147
4.2.5. Wnioski	149
4.3. Transfer dowodów zawierających dane osobowe w Unii Europejskiej	151
4.3.1. Europejski nakaz dochodzeniowy	153
4.3.2. Dowody elektroniczne	159
4.3.3. Wnioski	164
Podsumowanie	167
Bibliografia	171

WSTĘP

Standardy ochrony danych osobowych powinny być istotnym elementem każdej czynności podejmowanej w ramach pracy organów ścigania. To przekonanie stało u podstaw badań, których rezultatem jest niniejsza publikacja.

Celem rozważań przedstawionych w pracy jest ocena wpływu standardów ochrony danych osobowych na wybrane czynności organów ścigania, tj. inwigilację, automatyczne podejmowanie decyzji, profilowanie oraz przekazywanie danych w ramach współpracy dowodowej w Unii Europejskiej. Istotne jest ustalenie, czy i w jakim zakresie standardy ochrony danych osobowych mogą wpłynąć na czynności podejmowane przez organy ścigania, uzupełniając w tym zakresie krajowe przepisy, pomagając realizować standardy wynikające z orzecznictwa Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej oraz zastępując brakujące elementy współpracy unijnej.

Praca złożona jest z czterech rozdziałów i podsumowania. Rozdział I, mający w istocie charakter wprowadzenia, zawiera zwięzłą analizę ewolucji pojmowania danych osobowych i sposobu korzystania z nich w zwalczaniu przestępczości. Zasadnicze rozważania otwiera rozdział II poświęcony określeniu zakresu przedmiotowego i podmiotowego przepisów o ochronie danych osobowych jako pola badawczego dla części analitycznej pracy. W rozdziale III zaprezentowano standardy jakości ochrony danych, przedstawionych według systematyki jakości danych oraz jakości przetwarzania danych. Przyjęta metodyka służy uchwyceniu w zwięzłej formie najważniejszych elementów ochrony danych, w tym zwłaszcza zasad przetwarzania, praw jednostki i obowiązków admini-

stratorów. Elementy te mają kluczowe z kolei znaczenie dla dalszych rozważań w części dotyczącej konkretnych czynności podejmowanych przez organy ścigania. Analiza odbywa się zarówno na poziomie unijnym, jak i krajowym, co pozwala również określić stopień zgodności prawa krajowego z unijnym, a także kierunek uzupełniania niezgodności przez administratorów, również w ramach bezpośredniego stosowania dyrektywy 2016/680. W rozdziale IV przeanalizowano trzy szczególne formy pracy organów ścigania: a) inwigilację, b) automatyczne podejmowanie decyzji i profilowanie oraz c) transfer dowodów w Unii w ramach europejskiego nakazu dochodzeniowego i projektowanych instrumentów dotyczących dowodów elektronicznych. Wybór dwóch pierwszych czynności uzasadnia ich podatność na nowe technologie, co zwiększa znacząco ryzyko ich stosowania, w tym arbitralności ze strony organów czy nieuprawnionej ingerencji w prawo do prywatności. W pracy zbadano zatem, czy przepisy o ochronie danych osobowych mają potencjał redukujący towarzyszące tym czynnościom zagrożenia, przyczyniając się zarazem do wzrostu zaufania do pracy organów ścigania w Unii Europejskiej. Część dotycząca transferu dowodów w Unii była zaś analizowana z perspektywy braku we współpracy dowodowej zasady specjalności oraz roli, jaką ochrona danych osobowych może pełnić w wypełnieniu tej luki. W części tej ustalono również, które unijne przepisy o ochronie danych osobowych powinny mieć zastosowanie przy korzystaniu z europejskiego nakazu dochodzeniowego.

Osią prowadzonych w książce rozważań jest dyrektywa 2016/680 oraz, na gruncie krajowym, ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, a także, w odpowiednim zakresie, ustawy szczególne regulujące pracę organów ścigania, w tym w szczególności ustawa o Policji. Zamierzeniem podjętej pracy nie jest bowiem analiza porównawcza całego dorobku legislacyjnego i *soft law* w dziedzinie ochrony danych osobowych ani kompleksowy przegląd działań krajowych organów ścigania w tym kontekście. Z uwagi jednak na fakt, że niektóre z przyjętych w innych miejscach rozwiązań są relewantne również w niniejszej pracy, w odpowiednich częściach książki odniesiono się też do rozwiązań funkcjonujących w Eurojuście i Europolu, do orzecznictwa Europejskiego Trybunału Praw Człowieka,

Trybunału Sprawiedliwości Unii Europejskiej i Trybunału Konstytucyjnego, a także do ochrony danych osobowych w ramach RODO.

Badania, których wyniki przedstawiono poniżej, prowadzone były w ramach realizacji na Uniwersytecie im. Adama Mickiewicza w Poznaniu programu badawczego „Ochrona danych osobowych w procesie karnym w świetle gwarancji konstytucyjnych i prawa Unii Europejskiej” (NCN, program OPUS, nr 2015/19/B/HS5/00122, 2016–2020). Jego głównym wykonawcą jest dr Martyna Kusak.

3.2.1.2. Standard krajowy

Wymóg realizacji standardu w zakresie ochrony prawidłowości danych w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości ujęty został w treści art. 31 ust. 1 pkt 4 oraz art. 31 ust. 2. Te dwa przepisy łącznie oddają dosłownie treść art. 4 ust. 1 lit. d dyrektywy 2016/680. Podobnie jak w dyrektywie, również w analizowanej ustawie znalazły się przepisy konkretyzujące **obowiązek dbałości o prawidłowość danych**⁸.

Zgodnie z art. 31 ust. 2 u. zwal. przest. administrator podejmuje wszelkie działania, by dane osobowe, które są nieprawidłowe, w świetle celów przetwarzania zostały niezwłocznie usunięte lub sprostowane⁹. Rzeczywistą przesłanką weryfikacji prawidłowości danych będzie zatem, podobnie jak w dyrektywie 2016/680, **cel (cele) przetwarzania**. Jest to istotne o tyle, że dane można również przetwarzać w innych celach, zarówno mieszczących się w zakresie art. 1 pkt 1 u. zwal. przest., jak i tych wychodzących poza ten zakres (art. 4 ust. 2 dyrektywy 2016/680, art. 13 ust. 3 u. zwal. przest.), a wreszcie także w celach statystycznych i naukowych. W tym kontekście należy żałować, że ustawodawca nie zdecydował się na wprowadzenie terminu okresowego przeglądu gromadzonych danych według kryterium poprawności danych¹⁰. Tymczasem dziesięcioletni termin wskazany w art. 16 u. zwal. przest. odnosi się do obowiązku przeglądu danych jedynie w zakresie oceny zbędności tych danych, a nie *stricte* ich poprawności.

⁸ Obowiązek ten nie jest oczywiście nowością w polskim porządku prawnym; por. m.in. wyrok WSA w Warszawie z 2.04.2007 r., II SA/Wa 2328/06, LEX nr 319383, wydany w związku z art. 26 d. u.o.d.o. i dotyczący danych „merytorycznie poprawnych”.

⁹ W motywie 30 dyrektywy 2016/680 wskazano, że: „Zasadę prawidłowości danych należy stosować z uwzględnieniem charakteru i celu odnośnego przetwarzania”. Dalsza część omawianego motywu precyzuje, że istotna jest weryfikacja prawidłowości danych m.in. z uwagi na ich źródło i kontekst przetwarzania.

¹⁰ Przykładowo, w art. 6 ust. 1 reg. Eurojust znajduje się wymóg podejmowania wszelkich stosownych kroków, aby zapewnić usunięcie lub poprawienie błędnych lub niekompletnych danych, mając na uwadze cele, w jakich były one gromadzone i w jakich są w dalszym ciągu przetwarzane. Przepis ten, o ile również wprowadza weryfikację jakości w świetle celu, wyraźnie odnosi się też do aktualnego celu przetwarzania.

Jednym z najskuteczniejszych sposobów zapewnienia prawidłowości gromadzonych danych jest ich **ocena już na etapie zbierania**¹¹. Z tego powodu dyrektywa 2016/680 oparta jest na różnicowaniu, tak dalece jak to możliwe, danych osobowych opartych na faktach oraz danych osobowych opartych na indywidualnych ocenach (art. 7 ust. 1 dyrektywy 2016/680). Przepis ten został wdrożony w art. 20 u. zwal. przest., zgodnie z którym: „Przy przetwarzaniu danych osobowych administrator zapewnia rozróżnienie, o ile jest ono możliwe lub nie jest dalece utrudnione, na dane osobowe mające swoje źródło w faktach i dane osobowe mające swoje źródło w indywidualnych ocenach”. Zauważyć należy, że dokonując implementacji, ustawodawca wprowadził jednocześnie dodatkowe względem dyrektywy ograniczenie, używając sformułowania „nie jest dalece utrudnione”. Przepis ten nie ma rozwinięcia w przepisach dotyczących obowiązków administratora. Pozwala to pesymistycznie założyć, że korzystanie z niego może być marginalizowane w toku przetwarzania danych osobowych. Nakazuje jednocześnie sformułowanie postulatu **odzwierciedlenia potrzeby rozróżnienia obu kategorii danych w adekwatnym sposobie postępowania administratora danych, w tym oznaczenia danych**.

Szkoda, że ustawodawca ani w analizowanej ustawie, ani w ustawach ustrojowych nie wziął przykładu z rozwiązań **Europolu** dotyczących prawdziwości informacji, zgodnie z którymi **informację opisuje się według poniższych kodów oceny źródła (A–D) oraz oceny informacji (1–4)**:

- (A): gdy nie ma wątpliwości co do autentyczności, wiarygodności i kompetencji źródła lub jeżeli informacja jest dostarczona przez źródło, które okazało się rzetelne we wszystkich wypadkach;

¹¹ Por. rozważania w literaturze dotyczącej jakości informacji: T.C. Redman, *Chapter 2 – Measuring Data Accuracy — A Framework and Review* [w:] *Information Quality*, eds. R.Y. Wang, E.M. Pierce, S. Madnick, C.W. Fisher, London–New York 2005, <http://common.books24x7.com/toc.aspx?bookid=20757> (dostęp: 1.12.2019 r.); G.L. Rogova, *Information Quality in Fusion-Driven Human-Machine Environments* [w:] *Information Fusion and Data Science*, eds. É. Bossé, G.L. Rogova, Springer 2019, s. 10–13; C. Batini, M. Scannapieco, *Data and Information Quality. Dimensions, Principles and Techniques*, Springer 2016, s. 45.

- (B): gdy informacja dostarczona jest przez źródło, które w większości przypadków okazało się rzetelne;
- (C): gdy informacja dostarczona jest przez źródło, które w większości przypadków okazało się nierzetelne;
- (D): gdy nie można ocenić wiarygodności źródła;
 - (1): informacje, których prawdziwość nie budzi wątpliwości;
 - (2): informacje, które są znane źródłu osobiście, ale które nie są znane osobiście przekazującemu je urzędnikowi;
 - (3): informacje, które są znane źródłu osobiście, ale są potwierdzone przez inne informacje zarejestrowane wcześniej;
 - (4): informacje, które są znane źródłu osobiście i których nie można potwierdzić (art. 29 ust. 2 rozp. Europoł).

De lege ferenda administrator, używając systemu kodów na wzór tych z Europolu, mógłby opisywać dane osobowe, kierując się dbałością o ich prawidłowość. Z konkretnym kodem mogłaby zostać również połączona rewizja danych, na przykład wymóg częstszej aktualności tych danych o najbardziej wątpliwej jakości lub ograniczenia w dostępie czy dalszym przetwarzaniu. Takie działania w dużo większym zakresie aniżeli aktualne rozwiązania pozwoliłyby na realizację zasady prawidłowości danych i ostrożność w przetwarzaniu danych, których prawidłowość jest na niskim poziomie. Operowanie oparte na takiej jednolitej klasyfikacji byłoby również bez wątpienia pomocne w przekazywaniu danych osobowych przez służby objęte ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Usunięcie danych nieprawidłowych może nastąpić nie tylko na wniosek osoby, której dane dotyczą, lecz także z inicjatywy administratora. Zgodnie z art. 24 ust. 4 u. zwal. przest., jeżeli administrator stwierdzi z urzędu, że dane osobowe zostały zebrane lub są przetwarzane niezgodnie z przepisami niniejszej ustawy (a zatem również wtedy, gdy nie spełniają wyrażonego w art. 31 ust. 1 pkt 4 u. zwal. przest. wymogu prawidłowości), ma wówczas obowiązek usunięcia danych osobowych¹².

¹² Uwagi krytyczne uznające niniejszy przepis za *superfluum* w: *Ustawa o ochronie...*, red. A. Grzelak, s. 244.

Standardy weryfikacji jakości danych osobowych przed ich przesyłaniem lub udostępnianiem, o których mowa w art. 7 ust. 2 dyrektywy 2016/680, realizuje zaś art. 21 u. zwal. przest. Zgodnie z ust. 1 tego przepisu właściwy organ, przysyłając dane innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej, ma obowiązek uprzedniego zweryfikowania, w miarę potrzeby i możliwości, prawidłowości, kompletności i aktualności tych danych. Jak wynika z ust. 2 omawianego przepisu, przysyłając takie dane, przekazuje się również, w miarę potrzeby i możliwości, niezbędne dodatkowe informacje pozwalające temu odbiorcy ocenić stopień prawidłowości, kompletności oraz aktualności przesyłanych danych osobowych.

Wobec dyskrecjonalności decyzji wskazanych w art. 21 u. zwal. przest. w obu przypadkach warto postulować, aby **weryfikacja taka odbywała się głównie w stosunku do danych, których prawidłowość może rodzić wątpliwości, a także w świetle celu przetwarzania**. Inne ryzyko niesie bowiem przekazanie nieprawidłowego adresu świadka, a inne błędny numer rachunku bankowego podejrzanego, który inny organ zamierza monitorować. Pomocne w podejmowaniu decyzji może być kierowanie się podmiotem danych (art. 19 u. zwal. przest.), a także postulowane wcześniej operowanie kodami jakości danych. Tym sposobem można osiągnąć stan, w którym administrator podejmować będzie decyzję o potrzebie weryfikacji jakości danych osobowych przed przekazaniem, w oparciu o wcześniejsze zaklasyfikowanie danych połączone z informacją o ostatnim przeglądzie takich danych, lub przekazać odbiorcy informację o danych odtworzone na podstawie takiej klasyfikacji (np. informacje o ostatnim przeglądzie czy inicjalnym stopniu prawidłowości danych).

Postępowanie w przypadku **przesłania danych niekompletnych, nieprawidłowych lub nieaktualnych** lub przesłanych z naruszeniem przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości określa art. 21 ust. 3 tej ustawy. W takiej sytuacji właściwy organ, który przesłał dane, ma obowiązek bez zbędnej zwłoki poinformować o tym odbiorcę oraz:

- a) sprostować, uzupełnić lub uaktualnić te dane, a także przesłać temu odbiorcy dane właściwe, chyba że z uwagi na upływ czasu jest to oczywiście nieuzasadnione, albo
- b) usunąć lub ograniczyć przetwarzanie tych danych, a także poinformować o tym jego odbiorcę w celu usunięcia lub ograniczenia przez tego odbiorcę przetwarzania tych danych.

Ta ostatnia decyzja podejmowana jest w przypadku, gdy osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić, lub dane osobowe muszą zostać zachowane do celów dowodowych (art. 21 ust. 4 u. zwal. przest.).

W pierwszym przypadku zachodzi więc ciekawy na gruncie zastosowania omawianej ustawy przypadek, kiedy **wpływ na decyzję o przetwarzaniu ma podmiot danych**¹³. Aby był on realny, należy jednak posiadać wiedzę dotyczącą przetwarzania danych osobowych, samego rodzaju danych, ich prawidłowości oraz potencjalnej szansy ich dalszego przekazania. Może to być zatem uprawnienie trudne do zrealizowania w praktyce¹⁴.

Drugi przypadek, tj. **zachowanie danych w celach dowodowych, dotyczy przetwarzania polegającego na usuwaniu danych**. Wynika z niego, że danych nie usuwa się, lecz ogranicza się ich przetwarzanie, jeśli muszą być zachowane w celach dowodowych. Ponownie pomocne w tej sytuacji może być korzystanie z klasyfikacji prawidłowości danych połączonej z celem ich wykorzystania lub weryfikacją przed przekazaniem innym organom. Dane nieprawidłowe przetwarzane „awaryjnie” w celach dowodowych byłyby wówczas opatrzone specjalnym kodem, ograniczającym ich przetwarzanie w dalszych celach czy przekazywanie innym organom.

¹³ O ile oczywiście zachodzą pozostałe wskazane w tym przepisie przesłanki, tj. kwestionowanie przez osobę, której dane dotyczą, prawidłowości jej danych oraz brak możliwości sprawdzenia tej kwestii przez administratora.

¹⁴ Choć w unijnej współpracy obowiązuje już przepis angażujący osobę, której dane dotyczą, w proces dalszego przekazania tych danych; por. art. 23 ust. 1 lit. d konw. UE 2000.

Prezentowana publikacja jest spójnym opisem standardów ochrony danych osobowych w działaniach podejmowanych przez organy ścigania oraz ich wpływu na wybrane czynności, tj. inwigilację, automatyczne podejmowanie decyzji i profilowanie oraz przekazywanie danych w ramach współpracy dowodowej w Unii Europejskiej. Autorzy weryfikują, czy i w jakim zakresie standardy te mają potencjał realizować ochronę prawa do prywatności oraz zastąpić brakujące elementy współpracy unijnej w sprawach karnych.

Prowadzone w książce rozważania opierają się na przepisach m.in. ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz dyrektywy 2016/680, analizowanych z uwzględnieniem ustaw szczególnych regulujących pracę organów ścigania. Odniesiono się również do rozwiązań funkcjonujących w organizacjach Eurojust i Europol, do orzecznictwa ETPCz, TSUE i TK, a także do ochrony danych osobowych na podstawie RODO.

Książka jest przeznaczona dla osób zajmujących się procesem karnym oraz ochroną danych osobowych, a także funkcjonariuszy i administratorów danych osobowych w służbach zajmujących się ściganiem i zwalczaniem przestępczości. Będzie również cennym źródłem wiedzy dla uczestników postępowań karnych, a także studentów i aplikantów prawniczych.

Martyna Kusak – doktor nauk prawnych Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz Uniwersytetu w Gandawie (Belgia); adiunkt w Zakładzie Postępowania Karnego UAM, post-doc w Institute for International Research on Criminal Policy (Uniwersytet w Gandawie, Belgia). Specjalizuje się w europejskiej i międzynarodowej współpracy w sprawach karnych, ochronie prywatności i danych osobowych oraz prawnych aspektach big data, algorytmów i sztucznej inteligencji.

Paweł Wiliński – profesor doktor habilitowany nauk prawnych; kierownik Zakładu Postępowania Karnego Uniwersytetu im. Adama Mickiewicza w Poznaniu, sędzia Sądu Najwyższego orzekający w Izbie Karnej, sędzia ad hoc Europejskiego Trybunału Praw Człowieka (2010–2012, 2015–2016). W latach 2001–2017 pracownik Trybunału Konstytucyjnego. Członek Komisji Kodyfikacyjnej Prawa Karnego (2009–2015). Autor i redaktor około 200 publikacji naukowych.



9788381876322 W01P01

ISBN 978-83-8187-632-2



9 788381 876322

ZAMÓWIENIA:

INFOLINIA 801 04 45 45

ZAMOWIENIA@WOLTERSKLUWER.PL

WWW.PROFINFO.PL