

P
ME

3/2019

PRAWO

Mediów Elektronicznych

Prawa osób, których dane dotyczą, w świetle dyrektywy 2016/680

Damian Klimas

What are the most common legal bases for personal data processing in the context of local public authorities' activities? Legal obligation vs Public Interest

Denitsa Kozuharova, Dilyana Kutsarova

Możliwości obciążenia odpowiedzialnością za wypadek pojazdu autonomicznego a koncepcja stworzenia krajowego funduszu ubezpieczeń komunikacyjnych jako forma refundacji kosztów

Mikołaj Domagała

Doręczenia elektroniczne pomiędzy podmiotami publicznymi w postępowaniu

r.pr. Sylwester Szczepaniak

RADA PROGRAMOWA:

r.pr. Włodzimierz Chróścik
SNSA Jacek Czaja
adw. Rafał Dębowski
prof. Włodzimierz Gromski
prof. Ryszard Jaworski
adw. Xawery Konarski
prof. Michele Angelo Lupoi
prof. dr hab. Jacek Mazurkiewicz
prof. Vytautas Nekrošius
dr Grzegorz Sibiga
prof. Grażyna Szpor
prof. Andreas Wiebe
dr Wojciech Wiewiórowski
prof. Krzysztof Wójtowicz

www.ksiegarnia.beck.pl



Cena 65 zł (w tym 8% VAT)



PME

3/2019

Redakcja Kwartalnika Naukowego Prawo Mediów Elektronicznych

Redaktor naczelny: prof. dr hab. *Jacek Gołaczyński*, UWr
Sekretarz redakcji dr hab. prof. nadzw. UOp *Dariusz Szostek*
Członek redakcji dr hab. prof. nadzw. UOp *Piotr Stec*
Członek redakcji dr hab. *Marek Leśniak*, UWr
Członek redakcji dr *Aleksandra Klich*, USz

Rada programowa:

r.pr. *Włodzimierz Chrościk*
sędzia *Jacek Czaja*, NSA
adw. *Rafał Dębowski*
dr hab. prof. nadzw. UWr *Włodzimierz Gromski* (przewodniczący)
prof. dr hab. *Ryszard Jaworski*, UWr
adw. *Xawery Konarski*
prof. *Avv. Michele Angelo Lupoi*, Uniwersytet Boloński
prof. dr hab. *Jacek Mazurkiewicz*
prof. dr habil. *Vytautas Nekrošius*, Uniwersytet Wileński
dr *Grzegorz Sibiga*, INP PAN
dr hab. prof. nadzw. UKSW *Grażyna Szpor*
prof. dr *Andreas Wiebe*, University of Goettingen
dr *Wojciech Wiewiórowski*, UG
prof. dr hab. *Krzysztof Wójtowicz*, UWr

Recenzenci:

dr hab. prof. nadzw. UMK *Andrzej Adamski*
prof. *Zsolt Balogh*, Uniwersytet Corvinus Budapeszt
dr hab. prof. UŁ *Sławomir Cieślak*
dr hab. prof. nadzw. *Kinga Flaga-Gieruszyńska*, USz
prof. dr hab. *Jacek Górecki*, UŚ w Katowicach
prof. em. dr *Wolfgang Kilian*, University of Hannover
dr hab. prof. nadzw. UJ *Ryszard Markiewicz*
dr hab. *Marek Świerczyński*, UKSW
prof. *Richard Warner* Ph.D, Chicago – Kent College of Law
dr hab. prof. nadz. UŚ *Kazimierz Zgryzek*

Adres redakcji:

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl



Wydawca:

Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
fax: 22 33 77 602
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Prawa osób, których dane dotyczą, w świetle dyrektywy 2016/680 <i>Damian Klimas</i>	4
What are the most common legal bases for personal data processing in the context of local public authorities' activities? Legal obligation vs Public Interest <i>Denitsa Kozhuharova, Dilyana Kutsarova</i>	11
Możliwości obciążenia odpowiedzialnością za wypadek pojazdu autonomicznego a koncepcja stworzenia krajowego funduszu ubezpieczeń komunikacyjnych jako forma refundacji kosztów <i>Mikołaj Domagała</i>	17
Doręczenia elektroniczne pomiędzy podmiotami publicznymi w postępowaniu r.pr. <i>Sylwester Szczepaniak</i>	26

Contents

Rights of persons whose data regard directive 2016/680 <i>Damian Klimas</i>	4
What are the most common legal bases for personal data processing in the context of local public authorities' activities? Legal obligation vs Public Interest <i>Denitsa Kozhuharova, Dilyana Kutsarova</i>	11
The possibility to hold an entity liable for an accident of an autonomous vehicle and the concept of creating a national car insurance fund as a form of reimbursement of costs <i>Mikołaj Domagała</i>	17
E-delivery between public entities during a proceeding r.pr. <i>Sylwester Szczepaniak</i>	26

Szanowni Państwo,

z przyjemnością przedstawiam trzeci w 2019 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. Podobnie jak poprzednie numery, również ten został poświęcony zagadnieniom prawnym mającym związek z nowymi technologiami. Niezmiennie proponujemy współpracę i publikację artykułów, glos czy recenzji wszystkim tym autorom, którzy podejmują tematykę wpływu nowych technologii na prawo prywatne lub publiczne. Czasopismo ma charakter interdyscyplinarny i nie ogranicza się do jednej gałęzi prawa.

W bieżącym numerze prezentujemy m.in. opracowanie dotyczące praw osób, których dane dotyczą w świetle unijnej dyrektywy 2016/680 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. W bieżącym numerze znajdziecie Państwo także artykuł dotyczący możliwości obciążenia odpowiedzialnością za wypadek pojazdu autonomicznego w kontekście koncepcji stworzenia krajowego funduszu ubezpieczeń komunikacyjnych jako formy refundacji kosztów, jak również analizę prawnych możliwości utrwalania przebiegu czynności komornika sądowego za pomocą urządzenia rejestrującego obraz i dźwięk. Z uwagi na to, że kwartalnik Prawo Mediów Elektronicznych cieszy się popularnością także wśród zagranicznych autorów, również w tym numerze znajdziemy publikację obcojęzyczną poświęconą najczęstszym podstawom prawnym przetwarzania danych osobowych w kontekście działań lokalnych władz publicznych.

Zapraszamy do publikacji na łamach Prawa Mediów Elektronicznych, a także do kontaktu z nami pod adresem: pme@beck.pl.

Z poważaniem,
prof. dr hab. *Jacek Gołaczyński*

Prawa osób, których dane dotyczą, w świetle dyrektywy 2016/680¹

Damian Klimas²

Celem niniejszego opracowania jest przeanalizowanie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 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 uchyłająca Decyzję Ramową Rady 2008/977/WSiSW³, a także rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)⁴ w celu określenia praw osób, których dane dotyczą.

Uwagi wstępne

Dyrektywa 2016/680 jest najnowszym aktem prawnym UE w dziedzinie szczególnej ochrony danych osobowych, tj. w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar. Ten akt prawny, który wszedł w życie 5.5.2016 r., uchylił Decyzję Ramową 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych⁵. Dyrektywa traktowana jest jako *lex specialis* w zakresie ochrony danych osobowych w prawie karnym, podczas gdy RODO jest *lex generalis* dla ochrony danych osobowych. Dyrektywa 2016/680 jest postrzegana jako szerszy akt prawny niż uchylona Decyzja Ramowa 2008/977/WSiSW. Część praw wynikających z RODO pokrywa się z prawami podmiotów danych wynikających z dyrektywy (UE) 2016/680.

Osoba, której dane dotyczą, i jej prawa

1. Ograniczenia i wykonywanie praw osób, których dane dotyczą

W dyrektywie 2016/680 poświęcono jeden rozdział prawom osób, których dane dotyczą. Przede wszystkim należy wyjaśnić, jakie informacje należy udostępnić osobie, której dane dotyczą, zgodnie z prawem osoby, której dane dotyczą, czyli:

- dostępu do danych osobowych,
- ich sprostowania,
- usunięcia danych,
- ograniczenia przetwarzania danych oraz
- prawami w postępowaniu karnym.

Osoby, których dane dotyczą, powinny być również informowane, gdy ich prawa są ograniczone, w tym na jakiej podstawie. Ponadto należy podkreślić, że właściwy organ nadzorczy może wykonywać i weryfikować prawa podmiotów danych⁶.

Prawa osób, których dane dotyczą, określone w dyrektywie 2016/680 są podobne do praw przewidzianych w RODO. Aby zapoznać się z przeglądem praw osób, których dane dotyczą, należy przeanalizować poniższą tabelę, która pokazuje, że większość praw ma identyczny tytuł, choć są one ograniczone w porównaniu do tych w RODO. W odniesieniu do dyrektywy 2016/680 państwa członkowskie mogą nakładać ograniczenia w celu uniknięcia np. utrudnień w dochodzeniach lub postępowaniach karnych. Bardziej złożona analiza praw znajduje się poniżej.

¹ Niniejszy artykuł stanowi częściowe tłumaczenie *Review report on Directive 2016/680 at legal practitioners*: <http://informproject.eu/wp-content/uploads/2018/05/D2.5.pdf> (dostęp z 1.8.2019 r.).

² Autor jest asystentem i doktorantem w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Inspektor ochrony danych, prawnik, członek grupy roboczej ds. Internetu Rzeczy przy Ministerstwie Cyfryzacji.

³ O.J. L 119, p. 89–131; dalej jako: dyrektywa 2016/680.

⁴ Dz.Urz. UE L Nr 119, s. 1; dalej jako: rozporządzenie lub RODO.

⁵ Decyzja ramowa Rady 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych Dz.Urz. UE L Nr 350, s. 60–71; dalej jako: Decyzja Ramowa 2008/977/WSiSW.

⁶ Art. 12–18 dyrektywy 2016/680, chociaż GR Art. 29 uważa, że art. 12 dyrektywy 2016/680 zawiera jedynie obowiązek administratora/podmiotu przetwarzającego. Więcej informacji na temat niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa znajduje się w Opinii GR Art. 29 2017/258 (2016/680). Przyjęto 20.11.2017 r.

Tabela 1. Prawa osoby, której dane dotyczą, na podstawie dyrektywy 2016/680 i RODO

Prawa osoby, której dane dotyczą	Dyrektywa 2016/680	RODO
Prawo do informacji	Art. 12–14	Art. 12–13
Prawo dostępu	Art. 12–15	Art. 15
Prawo do sprostowania	Art. 16	Art. 16
Prawo do usunięcia (Prawo do bycia zapomnianym)	Art. 16	Art. 17
Prawo do ograniczenia przetwarzania	Art. 16	Art. 18
Prawo do przenoszenia danych	X	Art. 20
Prawo do sprzeciwu wobec automatycznego podejmowaniu indywidualnych decyzji	X	Art. 21–22

Ograniczenia prawa dostępu do danych osoby, której dane dotyczą, są określone w art. 15 dyrektywy 2016/680. Przepis ten pozwala państwom członkowskim przyjąć środki ograniczające prawo osoby, której dane dotyczą, do dostępu do danych, pod warunkiem że takie ograniczenie stanowi konieczny i proporcjonalny środek z przyczyn wymienionych w jego ust. 1.

Zwolnienia z podstawowych praw i uzasadnionych interesów osoby fizycznej powinny być stosowane jako wyjątek, a nie jako reguła, a pominięcie informacji może być dozwolone w ramach postępowania przygotowawczego tylko tak długo, jak takie ograniczenie stanowi konieczny i proporcjonalny środek⁷.

Pominięte informacje muszą, zgodnie z orzecznictwem TS, zostać przekazane, gdy już nie mogą zagrozić przeprowadzanym postępowaniom przygotowawczym⁸. Jeżeli prawo dostępu do danych osoby, której dane dotyczą, zostało ograniczone tylko częściowo, administrator powinien zapewnić dostęp do przetwarzanych danych osobowych i informacji wymienionych w art. 14 dyrektywy 2016/680. Celem tego obowiązku jest uświadomienie osoby, której dane dotyczą, o przetwarzaniu danych i umożliwienie weryfikacji zgodności z prawem tego przetwarzania. Obowiązek ten powinien być realizowany w jasny i zrozumiały sposób, aby umożliwić osobie, której dane dotyczą, poznanie tych danych, weryfikację ich prawidłowości oraz ustalenie zgodności z prawem ich przetwarzania. Realizacja tego obowiązku może przyjąć formę kopii przetwarzanych danych dostarczonej na trwałym nośniku⁹. Dyrektywa nie determinuje, kto powinien ponieść koszt nośnika, niemniej wydaje się, że powinno stosować się analogię do rozwiązań proponowanych w ramach dostępu do informacji publicznej¹⁰.

Jeżeli administrator chce w pełni ograniczyć prawo dostępu do danych, ma obowiązek poinformować o tym osobę,

której dane dotyczą, bez zbędnej zwłoki, na piśmie o odmowie lub ograniczeniu dostępu i wskazując powody takiego stanu rzeczy, tj. uzasadniając. Ponadto administratorzy powinni udokumentować faktyczne lub prawne powody takiej decyzji oraz informacje takie muszą zostać udostępnione organom nadzoru na żądanie¹¹.

Państwa członkowskie powinny zapewnić, że administratorzy zawsze zapewniają odpowiedź na wniosek o dostęp do danych oraz że w przypadku ograniczenia lub odmowy prawa dostępu do danych osoba, której dane dotyczą, otrzyma informacje dotyczące prawa do złożenia skargi do organu nadzorczego i szczegółowe dane kontaktowe tego organu ochrony danych lub możliwość skorzystania z środków prawnych¹².

Artykuł 12 dyrektywy 2016/680 stanowi, że państwa członkowskie mają przekazywać informacje osobom, których dane dotyczą, „w zwięzłej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka”. Istotą tego nowego przepisu jest zapewnienie, że wszystkie informacje przekazywane osobom, których dane dotyczą, dotyczą obowiązku wynikającego z dyrektywy 2016/680 i służą rzeczywistemu przekazywaniu takich danych i zapewniona jest przejrzystość przetwarzania, co zagwarantuje, że legalne przetwarzanie danych osobowych jest uczciwe.

Należy podkreślić, że istnieje różnica między bezpośrednim a pośrednim wykonaniem praw osób, których dane dotyczą. Zasadą jest bezpośrednie wykonywanie prawa przez osobę, której dane dotyczą. Możliwe jest także wykonywanie praw w sposób pośredni, kiedy pewne informacje o nałożonych ograniczeniach nie są dostarczane osobie, której dane dotyczą, w należyty sposób z uzasadnionych powodów. Ważne jest, aby pamiętać, że przepisy dotyczące praw osoby, której dane dotyczą, podobnie jak całość dyrektywy 2016/680, mają pełne zastosowanie w postępowaniu karnym¹³.

2. Informacje, które należy udostępnić osobie, której dane dotyczą

Artykuł 13 dyrektywy 2016/680 określa informacje, które należy przekazać osobie, której dane dotyczą, bez rozróżniania, czy są one uzyskiwane od osoby, której dane dotyczą,

⁷ Opinia GR Art. 29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

⁸ *Ibidem*, Opinia 1/15 TS w sprawie projektu umowy PNR między Kanadą a Unią Europejską, 26.7.2017 r.; zob. także wyrok TS z 21.12.2016 r. Tele2 Sverige, Watson i inni w sprawie.

⁹ Zob. motyw 43 dyrektywy 2016/680.

¹⁰ Por. wyrok WSA w Gdańsku z 1.10.2014 r., II SA/Gd 594/14, Legalis.

¹¹ Opinia GR Art. 29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

¹² *Ibidem*.

¹³ Protokół z piątego posiedzenia grupy ekspertów Komisji ds. rozporządzenia 2016/679 i dyrektywy 2016/680 z 18.1.2017 r.

i tworzy obowiązek dostarczania dodatkowych informacji przez administratora danych. Zapewnia to stosowanie jednolitych zasad dla wszystkich osób, których dane dotyczą, z wyjątkami dotyczącymi ochrony praw, takimi jak ochrona życia, ściganie przestępstw itp.

Przetwarzanie danych w ramach dyrektywy 2016/680 może czasami być wykorzystywane w sposób, który mógłby spowodować szkodę dla osoby fizycznej. Jest to ważne, ponieważ przetwarzanie danych w ramach dyrektywy skutkuje ograniczeniem wolności i praw jednostek. Może być także dokonywane bez świadomości o dokonywaniu tego przetwarzania osób, których dane dotyczą¹⁴.

Artykuł 13 ust. 1 lit. a)–e) dyrektywy 2016/680 dotyczy ogólnych informacji, które należy podać opinii publicznej, i określa informacje, które administrator musi udostępnić osobom, których dane dotyczą. Należy zauważyć, że w przepisie tym użyto sformułowania „udostępnianie” informacji. Informacje, które powinny zostać udostępnione osobie, której dane dotyczą (art. 13 ust. 1), to:

- tożsamość administratora;
- istnienie operacji przetwarzania;
- cele przetwarzania;
- prawo do złożenia reklamacji;
- istnienie prawa do żądania od administratora dostępu, poprawiania lub usuwania danych osobowych lub ograniczenia przetwarzania¹⁵.

Przykładami udostępniania informacji, o których mowa w art. 13 dyrektywy 2016/680, jest umieszczenie na stronie internetowej policji polityki prywatności czy wywieszenie polityki prywatności w odniesieniu do rejestracji broni palnej na tablicy łatwo dostępnej w budynku policji.

Artykuł 13 ust. 2 dyrektywy 2016/680 stosuje się w konkretnych przypadkach¹⁶ określonych w przepisach przez państwa członkowskie. Artykuł ten nakłada na administratorów obowiązek przekazania dodatkowych, dalszych, informacji umożliwiających osobie, której dane dotyczą, wykonywanie jej praw. Jak opiniuje GR29, wskazuje to na różnicę w podejściu, przy czym można argumentować, że obowiązek ten nie dotyczy niektórych danych, ale pewnej procedury przetwarzania i kategorii osób, których dane dotyczą, które mogą na nią wpływać (związane z „określonym przypadkiem”, o którym mowa w art. 13 ust. 2)¹⁷. Motyw 42 preambuły zawiera wytyczne dotyczące tej kwestii, przedstawiając cel takiego podejścia. Zgodnie z nim, w celu umożliwienia korzystania z danych, osoba, której dane dotyczą, powinna być dodatkowo poinformowana o podstawie prawnej przetwarzania oraz okresie przechowywania tych danych, jeśli takie dalsze informacje są niezbędne, biorąc pod uwagę szczególne okoliczności, w których dane są przetwarzane, w celu zagwarantowania rzetelnego przetwarzania w odniesieniu do osoby, której dane dotyczą. Innymi słowy, informacje, które należy podać, zgodnie z art 13 § 2, powinny być ukierunkowane na

osobę, której dotyczą dane, a zatem związane z „konkretnym przypadkiem”¹⁸, a nie nastawione na dane ogólne dostępne (publiczne).

Informacje, które należy przekazać osobie, której dane dotyczą, w konkretnych przypadkach (art. 13 ust. 2 dyrektywy 2016/680) to:

- podstawa prawna przetwarzania;
- okres, w którym dane osobowe będą przechowywane, lub, jeżeli nie jest to możliwe, kryteria stosowane do określenia tego okresu;
- w stosownych przypadkach kategorie odbiorców danych osobowych, w tym państwa trzecie lub organizacje międzynarodowe;
- w razie potrzeby dalsze informacje, w szczególności w przypadku zbierania danych osobowych bez wiedzy osoby, której dane dotyczą¹⁹.

Państwa członkowskie mogą przyjąć środki legislacyjne opóźniające, ograniczające lub pomijające zawarty w art. 13 ust. 2 dyrektywy 2016/680 obowiązek dotyczący informowania osoby, której dane dotyczą, w zakresie, w jakim jest to konieczne i proporcjonalne w celu uniknięcia jakichkolwiek uszczerbków określonych w ust. 3 tego przepisu. Wszelkie ustawodawcze środki muszą uwzględniać podstawowe prawa i prawnie uzasadnione interesy osoby, której dane dotyczą²⁰. Artykuł 13 ust. 4 i art. 15 ust. 2 dyrektywy 2016/680 nie zezwalają na ogólne ograniczenia praw do informacji i dostępu osób, których dotyczą dane²¹.

3. Bezpośredni dostęp jako zasada ogólna

Artykuł 14 dyrektywy 2016/680 uprawnia osobę, której dane dotyczą, do prawa do informacji odnoszących się do przetwarzania informacji dotyczących tej osoby, a także do prawa dostępu do danych osobowych przetwarzanych przez administratora. Informacje powinny być dostarczane bezpłatnie, bez zbędnego opóźnienia²². Prawo to podlega warunkom i ograniczeniom podobnym do tych wymienionych we wspomnianym art. 13 dyrektywy 2016/680. Artykuł 14

¹⁴ Opinia WP 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

¹⁵ Zob. art. 13 ust. 1 dyrektywy 2016/680.

¹⁶ *Ibidem*.

¹⁷ *Ibidem*.

¹⁸ Zob. art. 13 ust. 2 i motyw 42 dyrektywy 2016/680.

¹⁹ Zob. art. 13 ust. 2 dyrektywy 2016/680.

²⁰ Opinia GR Art. 29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

²¹ *Ibidem*.

²² Według GR Art. 29, administratorzy powinni udzielać informacji w odpowiedzi na wniosek złożony na podstawie art. 14 przez osobę, której dane dotyczą, tak szybko, jak to możliwe, jeżeli jest to wykonalne w ciągu jednego miesiąca. W celu uzyskania dalszych informacji zob. Opinia WP 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

przewiduje prawo dostępu do danych osobowych osobie, której one dotyczą. Przepis ten wynika z art. 12 lit. a) dyrektywy 95/46/WE z dodatkiem nowych elementów informacji dotyczących osób, których dane dotyczą, takich jak okres przechowywania, prawa do poprawienia, usunięcia lub ograniczenia przetwarzania danych czy prawo do złożenia skargi. Rodzaj informacji zawartych w prawie dostępu (art. 14 dyrektywy 95/46/WE) to:

- cele i podstawy prawne przetwarzania;
- kategorie danych osobowych;
- odbiorcy lub kategorie odbiorców, którym dane osobowe zostały ujawnione, w szczególności odbiorcy danych w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości przewidywany okres przechowywania danych osobowych lub, jeżeli nie jest to możliwe, kryteria stosowane do określenia tego okresu;
- istnienie prawa osoby, której dane dotyczą, do żądania od administratora poprawienia lub usunięcia danych osobowych lub ograniczenia ich przetwarzania;
- prawo do złożenia skargi do organu nadzorczego oraz dane kontaktowe właściwego organu;
- przekazywanie informacji na temat źródła przetwarzanych danych osobowych i wszelkich dostępnych informacji (wszystkie istotne informacje o tym, jak i w jakich okolicznościach administrator je otrzymał).

Jako przykład korzystania z prawa dostępu można wskazać *J. Doe*, świadka zbrodni, której dokonano w czerwcu 2018 r. Ten, będąc przesłuchanym podczas dochodzenia, chciał wiedzieć, czy jego dane będą nadal przetwarzane w 2020 r. (sprawa zamknięta w grudniu 2018 r.). Aby otrzymać taką informację, skontaktował się z inspektorem ochrony danych w policji, która posiadała jurysdykcję w danej sprawie. Inspektor jako osoba kontaktowa dostarczyła informacji dotyczących *J. Doe*.

4. Prawo do sprostowania lub usunięcia oraz ograniczenia przetwarzania

Artykuł 16 dyrektywy 2016/680 zawiera bardziej złożone przepisy dotyczące prawa do bycia zapomnianym/sprostowania/ograniczenia przetwarzania w przeciwieństwie do przewidzianego w art. 16–18 RODO.

Środki przewidziane w art. 16 dyrektywy 2016/680 określają ramy dotyczące działań związanych z przetwarzaniem, które obejmuje dokładne dane, co ma ogromne znaczenie dla skutecznego i sprawiedliwego zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar z jednej strony oraz dla prywatności osoby, której dane dotyczą, z drugiej strony. Przetwarzanie niepoprawnych danych może mieć niekorzystny wpływ na osobę, której dane dotyczą, dla-

tego dane należy poprawić, w szczególności w odniesieniu do faktów²³, a osoba, której dane dotyczą, zażądała sprostowania. Administratorzy mają również obowiązek usuwania danych osobowych oraz umożliwienia osobom, których dane dotyczą, uzyskania prawa do usunięcia danych osobowych, od administratora, gdy przetwarzanie ich narusza dyrektywę 2016/680²⁴.

Osoba, której dane dotyczą, ma prawo do usunięcia swoich danych, w przypadku gdy dane te są nieprawidłowe, przetwarzanie jest niezgodne z prawem lub narusza wymogi przetwarzania danych należących do specjalnych kategorii danych²⁵. Osoby, których dane dotyczą, mają prawo do poprawiania nieprawidłowych danych osobowych, które ich dotyczą, w szczególności gdy odnoszą się do faktów, a także, biorąc pod uwagę cele przetwarzania, prawo uzyskania uzupełnienia niekompletnych danych osobowych, w tym poprzez dostarczenie informacji uzupełniających²⁶.

Usunięcie danych osobowych jest wymagane, w przypadku gdy przetwarzanie narusza zasady dotyczące przetwarzania danych osobowych, jeżeli jest to niezgodne z prawem, narusza przepisy dyrektywy 680/2016 w sprawie przetwarzania szczególnych kategorii danych osobowych lub w przypadku danych osobowych, które muszą zostać usunięte, aby spełnić prawne zobowiązanie, któremu podlega administrator²⁷. GR29 stwierdza, że w przypadku żądania usunięcia danych osobowych administratorzy określone dane osobowe muszą przechowywać dla celów dowodowych i gdy prawidłowość danych osobowych jest kwestionowana przez osobę, której dane dotyczą, a prawidłowość ta nie może zostać ustalona, dyrektywa 2016/680 przewiduje prawo do uzyskania ograniczenia przetwarzania zamiast usuwania danych przez administratora²⁸.

Dyrektywa 2016/680 nie przewiduje *expressis verbis* prawa do ograniczenia odrębnego od prawa do usunięcia danych, jak to uregulowano w art. 18 RODO. Niemniej jednak motywy 47 i 48 dyrektywy 2016/680 wyraźnie wspominają o tym prawie. W związku z tym GR29 stwierdziła, że państwa członkowskie powinny rozważyć stworzenie takiego prawa dla osoby, której dane dotyczą, w ich ustawodawstwie krajowym, zarówno jako następstwo prawa do usunięcia danych, jak i jako odrębne prawo dla osób, których dane dotyczą i które

²³ Zob. motyw 46 dyrektywy 2016/680.

²⁴ Zob. art. 16 ust. 2 i motyw 47 dyrektywy 2016/680.

²⁵ Zob. art. 16 dyrektywy 2016/680.

²⁶ Zob. motyw 47 dyrektywy 2016/680; Opinia 29 2017/258 w sprawie niektórych kluczowych zagadnień dyrektywy w sprawie egzekwowania przepisów (2016/680). Przyjęto 20.11.2017 r.

²⁷ Opinia GR Art. 29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

²⁸ *Ibidem*. GR Art. 29 zaleciła udokumentowanie takich ograniczeń i wskazanie na przykład, kiedy ograniczenie zostało rozpoczęte i zatrzymane, ponadto w przypadku ograniczenia przetwarzania danych nie powinny one być wysyłane do innych administratorów, dopóki ograniczenie nie zostanie zniesione.

powinny móc poprosić o ograniczenie przetwarzania w innych przypadkach niż dwie sytuacje przewidziane w art. 16 ust. 3, szczególnie gdy administrator odmówi usunięcia danych bez ograniczania przetwarzania²⁹.

Artykuł 16 ust. 4 dyrektywy 2016/680 zapewnia również państwom członkowskim możliwość ograniczenia (w całości lub w części) pisemnych informacji, które należy przekazać osobie, której dane dotyczą, odnoszące się do odmowy administratora w zakresie sprostowania lub usunięcia danych, lub ograniczenia przetwarzania i przyczyn tej odmowy. Jeśli administrator odrzuci wniosek o usunięcie lub sprostowanie, będzie musiał dostarczyć pisemne informacje dotyczące odmowy oraz przyczyny odmowy.

Należy podkreślić, że chociaż dyrektywa przewiduje jedynie możliwość ograniczenia przetwarzania tych informacji na wnioski osoby, której dane dotyczą, w przypadku odmowy ze strony administratora, GR art. 29 podkreśla, że powinno być jasne, że w przypadkach, w których ustalono, że dane są niepoprawne lub niekompletne lub przetwarzane z naruszeniem art. 4, 8 lub 10 dyrektywy 2016/680, administrator danych nie może odmówić sprostowania lub usunięcia danych³⁰.

Podstawę dla państw członkowskich do ograniczenia prawa do sprostowania lub usunięcia danych (art. 16 ust. 4) stanowi:

- uniemożliwienie utrudniania czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
- uniemożliwienie zakłócania zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar;
- ochrona bezpieczeństwa publicznego;
- ochrona bezpieczeństwa narodowego;
- ochrona praw i wolności innych osób³¹.

Administratorzy powinni udzielić odpowiedzi na żądanie usunięcia lub sprostowania, a jeśli takie prawo podlega ograniczeniom lub nie jest stosowane, podmiot danych otrzymuje informacje dotyczące prawa do wniesienia skargi do organu nadzorczego lub wszczęcia postępowania sądowego³².

Wszelkie zwolnienia z podstawowych praw i uzasadnionych interesów osoby fizycznej nie powinny być stosowane z reguły i interpretowane w sposób restrykcyjny, jak regularnie przywołuje ETPCz, dotyczy to także ograniczenia praw podmiotów danych³³.

Administrator musi dopilnować, aby sprostowanie danych zostało przekazane pierwotnemu administratorowi, który zebrał dane osobowe, oraz wszystkim odbiorcom tych danych. Odbiorcy ci muszą również podobnie sprostować, usunąć lub ograniczyć przetwarzanie danych osobowych.

Można wskazać następujące przykłady korzystania z prawa do sprostowania lub usunięcia danych osobowych i ograniczenia przetwarzania:

- Sprostowanie: *J. Doe*, świadek przestępstwa do którego doszło w czerwcu 2018 r., został przesłuchany przez policję. *J. Doe* zmieniła nazwisko na Jones oraz adres, a także niedawno wyszła za mąż. Poinformowała policję o zmianie nazwiska i adresu. Policja poinformowała następnie właściwy w tej sprawie sąd kryminalny.
- Usunięcie: *J. Franco*, podejrzany o popełnienie przestępstwa we wrześniu 2018 r., został uznany za niewinnego stawianych zarzutów w styczniu 2019 r. Po pięciu latach złożył wniosek o usunięcie części swoich danych osobowych (specjalne kategorie), które zostały zebrane niezgodnie z prawem, a sąd karny potwierdził bezprawne zebranie danych podczas postępowania karnego.

5. Pośrednie wykonywanie praw osoby, której dane dotyczą

Podmiot danych ma prawo wykonywania swoich praw za pośrednictwem właściwego organu nadzoru (pośrednio). Taki pośredni dostęp do praw podmiotu danych jest możliwy, gdy:

- prawa osoby, której dane dotyczą, do informacji, dostępu lub informacji o odmowie sprostowania lub wymazanie zostały ograniczone przez administratora,
- na podstawie środków prawnych dopuszczających ograniczenia oraz gdy
- wyżej wymienionych uprawnień nie można było wykonywać bezpośrednio na rzecz administratora³⁴.

Pośrednie korzystanie z praw jest możliwe tylko wtedy, gdy pewne informacje na temat nałożonych ograniczeń nie zostały dostarczone osobie, której dane dotyczą, bez prawnie określonych powodów³⁵. Opcja posiadania uprawnień osoby, której dane dotyczą, wykonywanych przez właściwy organ, należy traktować jako dodatkową gwarancję oferowaną podmiotowi danych w kontekście Dyrektywy (UE) 2016/680. RODO nie przewiduje takiej możliwości, kiedy prawa osób, których dane dotyczą, będą ograniczone.

Administratorzy muszą informować osoby, których dane dotyczą, o możliwościach dochodzenia swoich praw za pośrednictwem organu nadzoru³⁶. Informacje administratora

²⁹ *Ibidem*.

³⁰ *Ibidem*. Ponadto GR Art. 29 zaleciła, aby państwa członkowskie zapewniły kategorie przetwarzania i sytuacje, w których kontrolerzy nie mogą nigdy, całkowicie lub częściowo, odmówić w celu usunięcia lub ograniczenia przetwarzania.

³¹ Zob. art. 16 ust. 4 dyrektywy 2016/680.

³² Opinia WP 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

³³ S. i Marper przeciwko Wielkiej Brytanii, ECHR 2008 lub MK przeciwko Francji, ECHR 2013.

³⁴ Opinia GR Art. 29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

³⁵ Protokół z piątego posiedzenia grupy ekspertów Komisji ds. rozporządzenia 2016/679 i dyrektywy 2016/680 z 18.1.2017 r.

³⁶ Zob. art. 17 ust. 2 dyrektywy 2016/680.

w odniesieniu do pośredniego dostępu powinny być jasne, zrozumiałe, przekazane podmiotowi danych tak szybko, jak to możliwe, przez administratora oraz zawierać dane kontaktowe właściwego organu nadzoru³⁷.

Właściwe organy nadzoru korzystające z praw „pośredniego dostępu” muszą przynajmniej informować osoby, których dane dotyczą, że wszystkie niezbędne weryfikacje lub przeglądy miały miejsce i że on lub ona ma prawo szukać środka prawnego³⁸.

Środki zaradcze, odpowiedzialność i kary – organy ochrony danych

Na podstawie dyrektywy 2016/680, a także RODO, każde państwo członkowskie ustanawia niezależny organ nadzorujący (organy ochrony danych, zwane dalej OOD), który będzie odpowiedzialny za monitorowanie stosowania dyrektywy 2016/680³⁹. Artykuł 50 dyrektywy 2016/680 przewiduje wzajemną pomoc między organami ochrony danych państw członkowskich. To jest rewolucja przepisów Decyzji Ramowej 2008/977/WSiSW, która nie przewidywała środków, które można by porównać z art. 50 dyrektywy 2016/680 w tym zakresie.

Dyrektywa 2016/680 daje osobom, których dane dotyczą, prawo do złożenia skargi do organu nadzorczego oraz prawo do otrzymania informacji o postępach, a także o wyniku skargi⁴⁰. Podmioty danych uzyskały prawo do sądowego środka odwoławczego przeciwko administratorowi lub podmiotowi przetwarzającemu⁴¹.

W dyrektywie 2016/680 określono ponadto, że organy ochrony danych mają skuteczne uprawnienia do prowadzenia postępowań (art. 47 ust. 1), skuteczne uprawnienia naprawcze (art. 47 ust. 2) i skuteczne uprawnienia doradcze (art. 47 ust. 3), a także uprawnienie do zgłaszania naruszeń przepisów przyjętych zgodnie z dyrektywą do organów sądowych oraz, w stosownych przypadkach, do rozpoczęcia lub podjęcia działań związanych z postępowaniem w celu egzekwowania przepisów przyjętych zgodnie z dyrektywą⁴².

W odniesieniu do uprawnień naprawczych, art. 47 ust. 2 dyrektywy 2016/680 przewiduje tylko przykłady tego, jakie mogą być te uprawnienia, takie jak nakazanie usunięcia lub sprostowania danych lub ograniczenia przetwarzania, w tym zakaz przetwarzania. W świetle GR29 ten atrybut wymaga związania uprawnień organów ochrony danych do ostrzeżenia, nakazania określonych działań naprawczych i wydawania wiążących decyzji przeciwko administratorowi⁴³.

Większość państw członkowskich będzie miała tylko jedno OOD zarówno dla RODO, jak i dyrektywy 2016/680, ale niektóre państwa członkowskie ograniczą uprawnienia swoich organów ochrony danych, gdy działają w zakresie dyrektywy⁴⁴.

Środki prawne przewidziane w dyrektywie 2016/680 to:

- Prawo do złożenia skargi do organu nadzorczego (art. 52);
- Prawo do skutecznego środka prawnego przed sądem od decyzji organu nadzorczego (art. 53);
- Prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu (art. 54);
- Prawo do bycia reprezentowanym (art. 55);
- Prawo do odszkodowania (art. 56).

Artykuł 55 dyrektywy 2016/680 stanowi, że osoby, których dane dotyczą, mają „prawo do umocowania organu, organizacji lub zrzeszenia o charakterze niezarobkowym, które zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych, do wniesienia w jej imieniu skargi”. Takie postanowienie umożliwia organizacjom o charakterze niezarobkowym specjalizującym się w ochronie praw osób, których dane dotyczą, bronienie osób, których dane dotyczą, w przypadku naruszenia danych. Taka organizacja specjalizująca się w obszarze obrony osób, których dane dotyczą, już istnieje i zapewnia pomoc tym osobom⁴⁵. Wspomniany przepis może być ważny z punktu widzenia prawników *pro bono*, którzy specjalizują się w ochronie danych osobowych, ponieważ prawodawca europejski otworzył nową niszę w zakresie udzielania osobom, których dane dotyczą, pomocy prawnej w odniesieniu do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar.

Artykuł 56 dyrektywy 2016/680 przewiduje odszkodowanie dla osób, które ponoszą szkodę w wyniku naruszenia spowodowanego niezgodną z prawem operacją przetwarzania lub jakimkolwiek działaniem naruszającym przepisy prawa krajowego przyjęte na mocy dyrektywy 2016/680. Każdy podmiot danych w tej sprawie jest uprawniony do otrzymania odszkodowania od administratora lub innego organu właściwego zgodnie z prawem państwa członkowskiego. Przepis ten jest bardzo podobny do art. 19 Decyzji Ramo-

³⁷ Opinia WP 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (UE 2016/680). Przyjęto 20.11.2017 r.

³⁸ *Ibidem*.

³⁹ Zob. art. 41 i 42 dyrektywy 2016/680.

⁴⁰ Zob. art. 52 dyrektywy 2016/680.

⁴¹ Zob. art. 53 i 54 dyrektywy 2016/680.

⁴² *Ibidem*.

⁴³ Opinia GR29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

⁴⁴ Protokół z siódmego posiedzenia grupy ekspertów Komisji ds. rozporządzenia 2016/679 i dyrektywy 2016/680 z 7.3.2017 r.

⁴⁵ Przykładowo: NOYB – Europejskie Centrum Praw Cyfrowych z siedzibą w Annagasse 8/8, 1010 Wiedeń, Austria, który został założony przez M. Schremsa – znanego działacza ds. prywatności.

wej 2008/977/WSiSW, który stanowi, że każda osoba, która poniosła szkodę w wyniku niezgodnej z prawem operacji przetwarzania danych lub w wyniku innego czynu niezgodnego z przepisami krajowymi przyjętymi zgodnie z Decyzją Ramową 2008/977/WSiSW, jest uprawniona do otrzymania odszkodowania za wyrządzoną szkodę od administratora danych lub innego organu właściwego zgodnie z prawem krajowym. Komisja Europejska stwierdziła (powołując się na orzecznictwo TSUE), że dostęp do odszkodowania nie może być oparty na wymogu winy po stronie administratora⁴⁶.

Dyrektywa 2016/680 nakazuje państwom członkowskim ustanowienie zasad dotyczących stosowanych kar w związku z naruszeniami przepisów przyjętych zgodnie z dyrektywą⁴⁷. W przeciwieństwie do art. 83 RODO dyrektywa 2016/680 nie zawiera przepisu dotyczącego kar administracyjnych, lecz jedynie art. 57, który odnosi się do „kar”. W motywie 89 stwierdza się, że można podlegać sankcjom – ale nie odnosi się do nich jako kar będących koniecznymi o charakterze przestępczym.

Podsumowanie

Niniejsza publikacja została stworzona w ramach projektu „Wprowadzenie reformy ochrony danych do systemu sądownictwa” (INFORM). Projekt ten jest finansowany z programu European Union's Justice Programme (2014–2020) w ramach Umowy o udzielenie dotacji nr 763866. Treść niniejszej publikacji przedstawia jedynie poglądy autora i jest jego wyłączną odpowiedzialnością. Komisja Europejska nie ponosi żadnej odpowiedzialności za wykorzystanie zawartych w niej informacji.

W kontekście raportu z analizy dyrektywy 2016/680 w odniesieniu do prawników – jednej z grup docelowych projektu

INFORM – ważne jest, aby po raz kolejny podkreślić, że nie ma żadnych obowiązków ani praw wynikających z dyrektywy 2016/680 skierowanych bezpośrednio do prawników. Niemniej jednak istnieją pewne aspekty dyrektywy, które mogą mieć wpływ na pracę prawników. Przykładowo należy wspomnieć o prawie do reprezentowania przewidzianym w art. 55 dyrektywy 2016/680. Osoba, której dane dotyczą, powinna być wyposażona w prawo do umocowania odpowiednich organów, organizacji lub zrzeszenia o charakterze niezarobkowym w celu złożenia skargi w jej imieniu i w ramach wykonywania jej prawa, o których mowa w art. 52, 53 i 54 dyrektywy 2016/680. Wspomniane przepisy stanowią nowe ramy zapewniania osobom, których dane dotyczą, pomocy prawnej odnoszącej się do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar.

Fakt, że prawnicy nie są wyodrębnionymi adresatami jako odrębna grupa docelowa w dyrektywie 2016/680, nie zmniejsza ich roli w dziedzinie ochrony danych. Prawnicy będący prawnymi przedstawicielami osób, których dane dotyczą, mogą być zobowiązani do ochrony prawa tych osób, co wynika z dyrektywy 2016/680. Zwłaszcza prawnicy, którzy reprezentują osoby fizyczne w dziedzinie prawa karnego⁴⁸, będą mogli zapewnić solidniejsze i dopasowane do indywidualnych potrzeb usługi prawne po przeczytaniu tego opracowania i monitorowaniu praw klienta określonych w dyrektywie 2016/680.

Praca naukowa finansowana ze środków finansowych na naukę w latach 2018-2019 przyznanych na realizację projektu międzynarodowego współfinansowanego.

⁴⁶ Protokół z siódmego posiedzenia grupy ekspertów Komisji ds. rozporządzenia 2016/679 i dyrektywy 2016/680 z 7.3.2017 r.

⁴⁷ Zob. art. 57 dyrektywy 2016/680.

⁴⁸ Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych oraz wykonywanie kar.

Słowa kluczowe: dyrektywa 2016/680, ochrona danych osobowych, dyrektywa policyjna.

Rights of persons whose data regard directive 2016/680

The purpose of this study is to analyze the directive 2016/680 of 27.4.2016 of the European Parliament and of the Council on the protection of natural persons in regard to processing of personal data by competent authorities in order to prevent crime, conduct preliminary proceedings, detect and prosecute criminal offences and execute penalties, in regard to the free movement of such data, and repealing the Council Framework Decision 2008/977/JHA and the regulation of the European Parliament and of the Council 2016/679 of 27.4.2016 on the protection of natural persons and the free movement of such data, and repealing the directive 95/46/EC (general regulation on data protection) in order to determine the rights of persons whose data is in question.

Keywords: directive 2016/680, personal data protection, law enforcement directive.

What are the most common legal bases for personal data processing in the context of local public authorities' activities? Legal obligation vs Public Interest

Denitsa Kozhuharova¹

Dilyana Kutsarova²

The current paper offers an overview on several provisions enshrined in Article 6 of the General Data Protection Regulation from the perspective of local public authorities. It advocates that administrative law notions might facilitate municipalities to make a better distinction when they process personal information either on the basis of legal obligation or for the performance of a task carried out in the public interest, or for the exercise of official authority vested in the controller. The paper reviews data subject rights implications in this relation. It also touches upon legitimate interests and consents applicability in day-to-day operations of personal data processing executed by local public authorities.

Introduction

The protection of personal data has become one of the central human rights over the last 20 years, given the increased importance and share of the data driven economy and the challenges that this imposes to an individual's privacy. The recent pan-European Data Protection Reform once more demonstrates the significant role of personal data protection by introducing considerable legislative measures to be applied throughout the entire European Union. The General Data Protection Regulation (GDPR) plays a major role in this respect. The Regulation entered into force on the 24th of May 2016, and is applied across member states since the 25th of May 2018.

Despite creating major buzz in the business ecosystem, the Regulation is equally applicable to the public sector as well. The Regulation envisages numerous measures aimed at enhancing the legal compliance of the public authorities' daily activities related to the processing of personal data in order to ensure the utmost respect to the right to data protection of natural persons.

However, a common feature of most of the public authorities in the EU is their insufficient readiness to face the challenges posed by the digital era, including the new data protection regime. And one of the most vulnerable public authorities are local public authorities which are exposed to continuous cyber-attacks which lead to data breaches and unlawful disclosure of personal data. In recent years there were many reported incidents in this regard – Dettlebach (Germany), Ooststellingwerf, Weststellingwerf and Opsterland (Netherlands), NotPetya (Ukraine). These cases illustrate general technical and administrative unpreparedness of local public authorities. Legal advisors employed by these institutions do not tend to be experts in the field of data protection.

Meanwhile, there are more than 30 000 local public authorities in the EU. Daily activities of local public authorities as data controllers presuppose wide interaction and processing of personal data. Therefore, they need to be aware and ready to provide adequate protection of personal data to ensure citizens that their fundamental right to personal data protection is respected. All these issues require immediate actions aimed at enhancing the understanding of local public authorities regarding their new obligations and needed steps to address them. Moreover, it requires an increase of knowledge of the administrative staff that is directly engaged with the processing of personal data.

This issue has inspired partners behind the Preparing local public authorities for the new data Protection Legislation (ProLegis) plan to design a project to answer to the training needs of local public authorities' employees that are to be engaged in personal data processing activities, regardless whether they have been appointed as Data Protection Officers or not. To this end, the ProLegis project is set to develop training materials and methodology that are tailored to the needs and expectation of local public authorities. The training materials are in the basis of all planned face-to-face and online training opportunities provided by the projects.

¹ Author is one of the key researchers with Law and Internet Foundation, responsible for the ProLegis project coordination. As a lawyer she was also involved in large-scale data protection implementation projects in the public sector, most notably the GDPR implementation by the Ministry of Education and Sciences. Beyond personal data protection & privacy, the other research fields she is engaged with are procedural rights, child rights and digital rights in general.

² Author graduated as LL.M. with honours from the University of Sofia, Faculty of Law in 2015. She has experience in delivering legal and ethical research products related to the implementation of ICT in the public and private sector. Her main field of expertise is data protection and cybersecurity law. Most of her work is related to the implementation and coordination of tasks within diverse EU funded projects targeting the enforcement of human rights through ICT tools.

In the course of the said training materials preparation, and later on – during the planned training events, many unclear points in the data protection regime have been identified. One of the recognised challenges that local public authorities meet is the precise definition of the legal basis for personal data processing. Although this question has been clarified in the materials prepared under the project, the authors of the current publication deemed that the issue requires further examination. To this end, the paper will discuss legal obligation and public interest as bases for lawful personal data processing. It will break down their essence and then contrast the major difference of their application by providing examples from day-to-day activities of the local public authorities. In order to provide robust examination, the paper will also touch upon the nature of legitimate interest, as well as upon the possibilities for municipalities to process personal data on the basis of citizens' consent.

The current paper was funded by the European Union's Rights, Equality and Citizenship Programme (2014–2020). The content of this publication represents views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The current paper introduces the vision of the authors on how the legal bases provided for in Article 6 pt. (c) and (e) of GDPR interrelate with the concepts of circumscribed powers and discretion deriving from administrative law. It should be noted that the reflections of the authors are mainly based upon the Bulgarian legal system and main terminological concepts.

Legal Obligation as a legal basis for personal data processing

1. What is to be understood as legal obligation?

According to art. 6, par. 1, pt. c GDPR, whenever personal data processing occurs pursuant to a legal obligation applicable to the controller it represents lawful processing. For example, this legal base would be applicable in cases where the controller processes personal information in relation to the applicable tax and social securities' regime, but also in scenarios where personal data is processed in the context of anti-money laundering procedures. Ultimately, what qualifies personal information processing under this particular legal ground is the fact that the controller does not make the decision whether to process personal data or not, they are obliged to do so by law. Here, the purposes of the processing are determined by the legislator, not by the controller. In fact, the controller is defined as such by the applicable law itself.

Thus, the assessment of whether such processing should take place at all is made by the legislator *a priori*, and the controller is the entity/person who is responsible to carry it out. It is to be noted here that only EU and Member State legislations could be the source of the legal obligation. The latter can never derive from a third country legal order, i.e. when the controller is subject to an obligation under the legislation of a third country, this processing cannot be justified in accordance to Art. 6, par. 1, pt. c.

With regards to the essence of the respective provision itself, Recital 45 of the GDPR clearly states that it is not necessary that the legal provision details the categories of personal data to be processed or concrete operations, but the provision of the general conditions themselves is considered sufficient. Moreover, it is presumed that the legislator has carried out a balancing test how the sought purpose of the processing relates to the rights and legitimate interest of the individuals, and whether the latter prevails, as long as all data protection principles as outlined by Art. 5 GDPR are observed³, including here also the proportionality and necessity test. In other words, it is presumed that the legislator, when adopting the respective provision, which envisages personal data processing, has already made an assessment on the necessity and proportionality of the processing. For local authorities this notion is particularly important, considering the legislative powers they may possess. However, it should be noted that depending on the particular data processing operation, the controller could be the one defining the appropriate means to achieve the purposes set by the law.

2. Why does this legal ground present a challenge to local public authorities as data controllers?

The nature of a legal obligation as a legal basis for personal data processing is quite clear to private sector controllers. The only case where they will process an individual's information as prescribed by the law would be precisely when they have to comply with a legal obligation applicable to them. They are not entities entrusted to enforce policies or realise public strategies. However, for the public sector controllers the situation is a bit more complex. Since public bodies, and local public authorities in particular, are bound to implement national, regional and local public policies, strategies, and action plans, it might pose an additional challenge to differentiate when personal data is processed in line with a legal obligation, and when this is done to fulfil a task of public interest or an

³ For more information, please visit: Working Party 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (access from 30.10.2019).

exercise of official authority. The fact that both legal bases are often commonly addressed in the GDPR (i.e. Recital (45), Recital (51), Recital (65)) produces further confusion to the local public authorities. The clear definition of the legal base in such a scenario is of utmost importance since this impacts data subject rights and their possible exercise and limitations.

An easy way to figure out whether the processing is carried out in order to comply with a legal obligation is for the controller to pose the question whether the respective legal provision is imperative or dispositive. If the law requires the controller to complete a certain activity and leaves no room for independent decision on their side, then the processing would take place under Art. 6, par. 1, pt. c GDPR – the processing is necessary for compliance with a legal obligation to which the controller is subject. Otherwise, if the law empowers the controller to decide how to act, then pt. e should be considered as the applicable legal basis.

Additionally, it could also be useful to examine if the controller acts with a level of discretion in relation to the particular processing operation or acts within circumscribed powers. Although this concept derives from administrative law theory, it is a quick method for local public authorities to assess which is the legal ground for a particular processing operation. In this context, one could rightfully pose the question whether each personal data processing operation occurring within circumscribed powers is falling into the scope of the provision of Art. 6, par. 1, pt. c GDPR. A public body might act within circumscribed powers pursuant to a provision deriving from primary or secondary legislation, but also whenever acting upon an order issued by a higher authority⁴, according to the Bulgarian administrative law's understanding. Thus, how could following an order be considered as compliance with a legal obligation? Firstly, it should be noted that in line with the administrative legal theory, only an individual on an executive position with an administration is to be considered as administrative authority, and the administration itself is given a supporting role implementing the authority's decisions. Moreover, GDPR itself clearly provides in Art. 29 that the persons acting under the authority of the controller process personal data solely under the instructions given by the controller.

Public Interest & Exercise of official authority as a legal basis for personal data processing

1. What is the essence of this legal ground for the processing of personal information?

Another commonly applied legal ground for personal data processing by the local public authorities is the one out-

lined by art. 6, par. 1, pt. e GDPR, which actually contains two separate basis – the personal data processing is related to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In order to determine whether a controller is able to use this legal base to ground their personal information processing activities, one should examine if the public task/the official authority are outlined, again, in the relevant legislation. It should be noted here that only EU or Member State legislation could serve as a ground for the public task/official authority exercise. In contrast with the legal obligation, the nature of the legal provision establishing the public task/vesting the official authority should be discretionary, enabling the controllers to take a motivated decision on a certain action. The public task/official authority might be also defined in policy documents, i.e. they might be incorporated in strategy, road maps, action plans, adopted in accordance to the national law, etc., outlining authorities' and other relevant actors' prerogatives in relation to a certain societal issue. These strategic documents might be issued on a national or regional, and even local level, targeting issues from a different severity or importance. What is important here is that there should be a legal provision entrusting a particular controller (in our case a local public authority) to carry out the respective policy/task. When the implementation of these policies does also include personal data processing its legal foundation will be the performance of a public task/the exercise of an official authority. Similarly, to what has been stated in the previous section, third-country legislation is never to be considered as a legal basis for personal data processing pursuant to Art. 6, par. 1, pt. e GDPR.

Examples of processing related to the performance of a task carried out in the public interest are different information and communication campaigns carried out by municipalities in order to raise awareness on environmental issues, or an assessment of the percentage of the population using different lines of public transport. What would fall under the scope of the exercise of official authority vested in the controller are, for instance, the decrees of a mayor issuing a fine or another administrative measure towards a citizen or a company which violates the municipal orders.

At the same time, it is possible that this legal ground is used not only by public authorities, but by private entities as well, as long as they are entrusted to implement partially or completely state policies. These are the cases where private organisations are procured to deliver social services, or support a municipality in the maintenance of public infrastructure as libraries, sport centres, etc.

⁴ I.e. Decision 258/26.3.2008, Blagoevgrad Administrative Court; Decision 70/26.7.2017, Shumen Administrative Court; Decision 150/10.7.2018, Yambol Administrative Court.

2. Why does this legal base present a challenge to local public authorities?

At a first glance, it might seem that the scope of application of this legal basis for personal data protection could be interpreted more broadly, ultimately establishing a more liberal regime to controllers. Nonetheless, this provision is to be interpreted and applied in a limitative manner. Although this legal basis could provide for a better flexibility of the controllers, a careful assessment is to be made on case-by-case basis to examine whether the public interest actually does prevail over the individual's one. This assessment might be made on the stage of legislation/strategic documents drafting, as again the legal provision can determine the purposes of processing.

However, this does not preclude the responsibility borne by the controller – a balancing test is still to be executed. Why is that? Going back to the presented relation between personal data processing pursuant to a legal obligation and circumscribed powers, it is clear that a comparable correlation is to be sought here as well. Furthermore, turning to administrative law theory, the notion of discretion seems appropriate to illustrate the nature of the responsibility that controllers are entrusted to bear. In accordance with the wider flexibility presented in the current section to which the local public authorities are entitled, and the necessity for local public authorities still to carry out an assessment, it is right to say that whenever they act upon discretion and this includes personal data processing, the latter is regulated by the provision of Art. 6, par. 1, pt. e GDPR.

From a practical point of view, this represents a challenge to local public authorities, as on the one hand – legal obligation and task carried out in the public interest/exercise of official authority, are regarded *en bloc* by the GDPR in numerous instances. On the other hand, the delimitation line between an imperative provision establishing a legal obligation and a dispositive provision outlining the margin of an official authority could be difficult to draw. To facilitate this process, whenever a local public authority is processing an individual's information, as a first step, it should be established whether this activity falls under the scope of discretion or circumscribed powers. From there on, municipalities would be able to easily identify the applicable legal bases for personal data processing as outlined by the GDPR, and address data subject rights exercise requests accordingly.

Data subject rights implications

The new data protection regime, and the GDPR in particular, continue the philosophy enshrined by the previous of EU act regulating this field – Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, by put-

ting the individual in the centre, enabling him/her to exercise control over the way their personal data is being handled. This is particularly valid in situations where private sector organisations and information service providers might be tempted to go a step beyond the promised data processing and use personal information in a non-transparent manner to curate products and services, or even manipulate citizens. Therefore, the new, enhanced set of rights available to citizens' disposal plays a significant role in holding these controllers accountable.

At the same time, public sector controllers, and local public authorities in particular, are bound to function in a transparent manner. They are the ones who forge the relationship of trust between the citizens and the government institutions. However, the legal regime applicable to them is quite different to the one that regulates the function of the private sector. Since local public authorities are a subject to imperative legal order and are required to implement state policies, they are obliged to keep a detailed track showcasing the consecutive execution of their activities. There is a limited number of situations where local public authorities would process data outside their capacity of governmental institutions.

On a practical level, however, the difference between legal obligation and task carried out in the public interest/exercise of official authority is to be made namely in relation to data subject rights. Personal data processing pursuant to both legal bases is providing for more limited application of data subject right. Still, whenever personal information is treated in accordance with Art. 6, par. 1, pt. e GDPR, the individual has a wider range of possibilities at his/her disposal.

But which data subject rights could be limited? Firstly, the right to information might be narrowed down. In cases where the personal data is not collected directly from the data subject, but *ex officio*⁵, local public authorities are not obliged to inform citizens pursuant to Art. 14 GDPR. This means that they are not required to disclose to citizen details such as the purposes of personal data processing, the categories of personal information which are being handled and for how long, where the data originated and to whom it is disclosed, including also transfers to third countries or international organisations. If a local public authority is implementing automated decision-making technologies, and if the personal information is collected *ex officio*, it is not mandatory that this information is made available to data subjects. Through this approach the responsibility to assess how the individual interest relates to the public one is borne by the legislator – as Art. 14, par. 5, pt. c of GDPR states that the non-disclosure of information to data subjects is only possible when the law

⁵ Article 14, par. 5, pt. c GDPR.

provides appropriate measures to protect the data subject's legitimate interests.

Furthermore, the right to erasure is also of limited application in cases where personal data is being processed pursuant to the compliance with legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The functioning of local public authorities may be compromised in an event of personal data deletion. As it was aforementioned, the nature of governmental institutions activities requires them to keep detailed track on the on-going and already executed procedures. Therefore, the EU legislator has very rightfully recognised this risk and inserted the provision of Art. 17, par. 3, pt. b GDPR, to prevent the impediment of public bodies' work.

The most drastic difference between the legal regime of the legal bases analysed in the current paper comes from the provision of Art. 21 GDPR. The right to object is a powerful tool available to natural persons to hold controllers accountable. It enables them to challenge any processing operation as long as it is based on the controller's legitimate interest or is done for the performance of a task in the public interest or for the exercise of official authority vested in the controller. When this right is exercised, the controller (or the local public authority in this case) has to demonstrate how the public interest overrides the individual's, otherwise the processing should cease. This is why it is of primordial importance for local public authorities to make a clear distinction between the processing operations executed in accordance with Art. 6, par. 1, pt. c, and those pursuant to Art. 6, par. 1, pt. e. This way, when a municipality is met with such a request, they would easily make an assessment to satisfy or refuse it, providing appropriate argumentation.

The Notion of legitimate interest

Although the idea of the current paper is to compare the scopes of two of the legal grounds established by Art. 6 of the GDPR in the context of local public authorities' activities, the essence of Art. 6, par. 1, pt. f is to be briefly examined to provide a comprehensive picture. While legitimate interest as a ground for personal data processing is never to be applied in relation to the provision of public services⁶, there are cases where it could serve as a basis to handle personal information. Local public authorities do not function solely as governmental institutions. They are also employers and contractors, and in this position their behaviour is regulated by private, and not public law. When acting in such capacity, it is possible that the personal data processed is linked to their legitimate interest. For example, in the case of on-going employment relationship, a local public authority might implement access control and video surveillance among other security meas-

ures. This operation of personal data processing would fall under the scope of its legitimate interest. Another example for the applicability of the said legal ground would be a court dispute with a contractor. In this scenario the information is once again processed pursuant to the legitimate interest of the local public authority. It is important to make the distinction in which capacity the local public authority acts, so data subject rights are appropriately managed, and citizens trust the governmental sector.

And what about the consent?

Around the 25th of May 2018, a lot of the public debates on data protection revolved around consent. In addition to that, users of variety of platforms were bombarded with emails to re-affirm their consent. And then suddenly, consent forms were pushed everywhere – in electronic environment, but also on the spot, in relation to the provision of services, regardless whether they are public or not. A person would go to their dentist, and even a hair dresser, and they would ask for their consent in order to perform services. The misunderstanding was so great that the Bulgaria Commission for Personal Data Protection issued a list with activities where personal data processing is never based on consent⁷. Although the mission of the present paper is to shed further light into the complex issue of the delimitation between personal data processing pursuant to a legal obligation and the one done in the public interest, the authors think it is quite necessary to highlight why consent cannot be the legal basis for personal data processing in the context of the local public authorities' activities.

Even though the data subject consent is listed first in the enumeration provided by art. 6, par. 1 of GDPR, this should not be understood in the sense that this is the main legal base for personal data processing that controllers have at their disposal. On the contrary – controllers and processors should resort to obtain natural persons' consent in the limited situations where there is no other legal basis present and where their legitimate interest would not override the individual's one. As it is outlined above, local public authorities would mainly process personal data either on the basis of a legal obligation, to which they are subject, or in accordance with the public interest. Practices where, for example, municipalities seek citizens' consent to enter personal data in a public registry, or for the purposes of participation in elections, should be abandoned.

⁶ Art. 6 par. 2 GPDR.

⁷ For more information, please visit: List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679, <https://www.cdpd.bg/en/index.php?p=element&aid=1186> (access from 30.10.2018).

In a very limited amount of cases a municipality might employ consent as a legal basis to process citizens' personal information. For instance, if a local public authority administration maintains an electronic newsletter, then the consent of the subscribers would be the legal base for its regular distribution.

Conclusion

At first glance, it might seem easy to differentiate which legal basis enshrined in Art 6, par. 1 of GDPR is applicable. However, on a practical level public sector controllers, and local public authorities in particular meet obstacles determining whether their activities are to be regulated under Art 6, par. 1 pt. c or pt. e. The situation is further tangled by the popular understanding of consent as the legal ground for personal data processing, and wide applicability of legitimate interest in the private sector. The current paper tries to solve this complex situation by offering a simple assessment based upon administrative law theory – whether the authority acts within circumscribed powers or discretion. This assessment would facilitate local government bodies to identify whether a certain processing operation is based on the compliance with legal obligation or falls under the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.

To this end, whenever personal data is processed upon a legal obligation, it should be noted that the controller has

no legal possibility to decide, nor discretion whether or not to carry out the processing. The law imposing such an obligation could be of primary or secondary nature detailing what kind of personal information is the object of the processing, and what is the specific purpose pursued. On the other hand, whenever a local government organisation has a room to decide whether and how to carry out an activity within its capacity as public body entrusted to implement laws and policies, any personal data processing in this relation would fall under the scope of Art. 6, par. 1, pt. e GDPR. In cases when they are able to act upon a discretion, a local public authority will process the personal data for the performance of a task in the public interest or for the exercise of an official authority.

Last but not least, the paper provides for an examination of the applicability of other legal bases for personal data processing by the local public authorities. The analysis also deduces that scenarios where local governments' actions are regulated by private law are not to be ignored. Thus, it is reasonable to consider their legitimate interest as a basis to handle personal information. Still, a clear distinction between these activities should be in place to enhance citizens' trust and provide for better data subject rights management. Consent is also reviewed from this point of view, stating its narrow applicability in the context of local government – only in case when a municipality carries out an atypical activity which is neither funded in law nor pursuant to its legitimate interest.

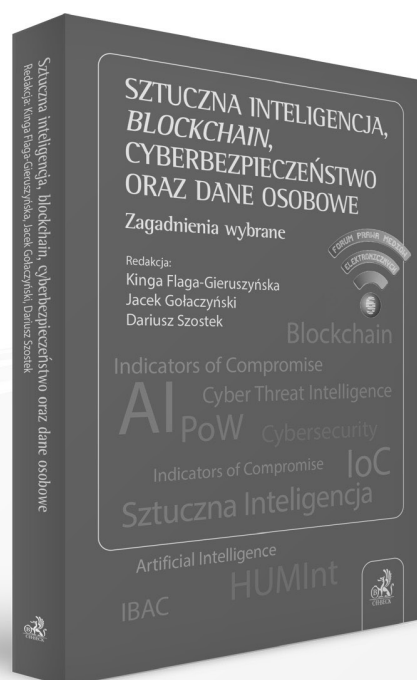
Key words: data protection, privacy, GDPR, legal bases, public interest, legal obligation.



Blockchain

www.ksiegarnia.beck.pl

Zadzwoń: 81 46 13 300 • E-mail: kontakt@beck.pl



Możliwości obciążenia odpowiedzialnością za wypadek pojazdu autonomicznego a koncepcja stworzenia krajowego funduszu ubezpieczeń komunikacyjnych jako forma refundacji kosztów

Mikołaj Domagała¹

Przedmiot niniejszego artykułu stanowi analiza możliwości stworzenia krajowego funduszu ubezpieczeń komunikacyjnych finansowanego ze składek opłacanych przez podmioty korzystające z pojazdów autonomicznych. Fundusz zarazem stanowiłby formę refundacji kosztów, a osoby, które odniosłyby szkody w wyniku zdarzenia, chcąc uzyskać rekompensatę z tytułu powstałych obrażeń ciała lub uszkodzeń mienia, mogłyby zwracać się bezpośrednio do funduszu. Zarazem autor prezentuje możliwości obciążenia poszczególnych podmiotów odpowiedzialnością cywilną za szkodę wynikłą na skutek wypadku samochodowego spowodowanego przez pojazd autonomiczny.

Uwagi wstępne

Jeszcze do niedawna samochód autonomiczny wydawał się jedynie wizją producentów filmów podejmujących problematykę futurystycznych technologii. Jednakże obecnie, w związku z niezwykle szybkim rozwojem nowoczesnych technologii, coraz więcej państw² decyduje się na udostępnianie producentom pojazdów zautomatyzowanych dróg publicznych w celu prowadzenia na nich prac badawczych w zakresie autonomizacji. Również w Polsce na podstawie przepisów ustawy z 11.1.2018 r. o elektromobilności i paliwach alternatywnych³ stworzono ramy prawne celem umożliwienia testowania pojazdów autonomicznych. Wraz z wejściem w życie przywołanego aktu w ustawie z 20.6.1997 r. – Prawo o ruchu drogowym⁴ dodano oddział odnoszący się do wykorzystania dróg na potrzeby prac badawczych nad pojazdami autonomicznymi.

Google LLC szacuje, że dzięki wprowadzeniu do powszechnego użytku samochodów autonomicznych niemal całkowicie zostaną wyeliminowane błędy ludzkie wpływające na zaistnienie wypadków samochodów w ogólności, co ostatecznie doprowadzi do zmniejszenia liczby wypadków samochodowych nawet o 90%⁵. Co prawda dane wskazywane przez Google wydają się przybierać nader optymistyczny charakter, jednak jest wielce prawdopodobne, że bez względu na to, w jak wysokim stopniu będzie zmniejszała się ogólna liczba wypadków samochodowych, korzystanie z pojazdów autonomicznych zmniejszy odsetek wypadków spowodowanych przez ludzi, jednocześnie zwiększając odsetek wypadków stanowiących przejaw wad produktu bądź usterek w jego działaniu. Aktualnie około 94% wypadków z udziałem samochodów stanowi wynik błędu ludzkiego, podczas gdy mniej niż 6% stanowi konsekwencję wad produktu⁶. Jednak, jak wskazuje się w najnowszych raportach, w nowej, zdomi-

nowanej przez pojazdy samojezdne rzeczywistości zaprezentowane proporcje ulegną odwróceniu.

Jednocześnie przewiduje się, że z uwagi na wysokie koszty posiadania prywatnych pojazdów autonomicznych coraz mniej popularne stanie się posiadanie samochodów prywatnych, a na popularności zyska system bazujący na wspólnym korzystaniu z pojazdów osobowych przez większą liczbę osób (ang. *car-sharing*⁷ lub *car-pooling*⁸). Podmioty specjalizujące

¹ Uniwersytet Opolski. Centrum Prawnych Problemów Techniki i Nowych Technologii.

² Zob. T. Litman, *Autonomous Vehicle Implementation Predictions. Implications for Transport Planning*, Victoria Transport Policy Institute, 24.7.2018 r., <https://www.vtpi.org/avip.pdf> (dostęp z 25.9.2018 r.).

³ T.j. Dz.U. z 2019 r. poz. 1124 ze zm.

⁴ T.j. Dz.U. z 2018 r. poz. 1990 ze zm.

⁵ C. Mui, *Fasten Your Seatbelts: Google's Driverless Car is Worth Trillions* (Part 1), Forbes, 22.1.2013 r., <https://www.forbes.com/sites/chunka-mui/2013/01/22/fasten-your-seatbelts-googles-driverless-car-is-worth-trillions-ns/#1448a45f79dd> (dostęp z 25.9.2018 r.).

⁶ G.E. Marchant, R.A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, Santa Clara Law Review 2012, vol. 52, No. 4, s. 1321–1340.

⁷ System wspólnego użytkowania samochodów osobowych funkcjonujący w ponad 600 miastach na świecie. Samochody są udostępniane za opłatą użytkownikom przez operatorów floty pojazdów, którymi są różne spółki, agencje publiczne, spółdzielnie, stowarzyszenia lub grupy osób fizycznych. Stosowanie tego systemu zwiększa intensywność wykorzystania pojazdów w ciągu doby, co prowadzi do zahamowania wzrostu liczby samochodów rejestrowanych prywatnie; Słownik pojęć Strategii rozwoju transportu do 2020 r. (z perspektywą do 2030 r.), Ministerstwo Infrastruktury, <https://www.gov.pl/infrastruktura/strategia-rozwoju-transportu-do-2020-roku-z-perspektywa-do-2030-roku> (dostęp z 25.9.2018 r.).

⁸ System upodobniający i dostosowujący samochód osobowy do transportu zbiorowego. Polega na zwiększaniu liczby pasażerów w czasie przejazdu samochodem, głównie poprzez kojarzenie osób dojeżdżających do pracy lub nauki na tych samych trasach. Jest rozwijany w sytuacjach, gdy ze względu na małe natężenie ruchu nieopłacalne jest uruchamianie linii zorganizowanego transportu zbiorowego. Funkcjonuje na bazie społecznościowych portali internetowych lub tablic informacyjnych w miejscu pracy; Słownik pojęć Strategii rozwoju transportu do 2020 r. (z perspektywą do 2030 r.), Ministerstwo Infrastruktury, <https://www.gov.pl/infrastruktura/strategia-rozwoju-transportu-do-2020-roku-z-perspektywa-do-2030-roku> (dostęp z 25.9.2018 r.).

się we współużytkowaniu samochodów będą dysponowały flotą pojazdów autonomicznych, które osoby zainteresowane będą mogły wynająć zgodnie z własnymi potrzebami, podając swoją lokalizację, cel podróży oraz czas niezbędny na dotarcie do celu⁹. Warto przy tym zaznaczyć, że rynek europejski, na którym funkcjonuje 6 milionów użytkowników poruszających się 70 000 samochodami, odpowiada za niespełna 50% globalnego rynku usług typu *car-sharing*. Krajem, w którym usługa jest najbardziej rozwinięta, są Niemcy, gdzie z systemu korzysta 1,7 milionów mieszkańców z 597 miast i gmin na terenie całego kraju¹⁰.

Co do zasady, z uwagi na stopniowe pojawianie się na drogach coraz większej liczby pojazdów autonomicznych ogólna liczba wypadków drogowych powinna maleć. Powinniśmy jednak pamiętać, że liczba kolizji nie zostanie zredukowana do poziomu zerowego, a zaistniałe zdarzenia przybiorą zgoła odmienny od dotychczasowych charakter, w związku z czym obecnie funkcjonujący system odpowiedzialności cywilnej oparty na obowiązkowym ubezpieczeniu odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych za szkody powstałe w związku z ruchem tych pojazdów, dobrowolnym ubezpieczeniu następstw nieszczęśliwych wypadków (tzw. ubezpieczenie NW) oraz dobrowolnym ubezpieczeniu szkód powstałych w pojeździe i jego wyposażeniu (tzw. ubezpieczenie AC) może nie sprostać odmiennościom powstałym w związku z pojawieniem się na rynku pojazdów autonomicznych.

Podmioty ponoszące obecnie odpowiedzialność cywilną

W praktyce nierzadko zdarza się, że kierowca pojazdu mechanicznego nie jest jednocześnie jego posiadaczem. Dlatego też istnieje potrzeba zdefiniowania nie tylko wzajemnych praw, ale też obowiązków w relacjach istniejących pomiędzy poszkodowanym, kierowcą oraz posiadaczem pojazdu.

Wobec poszkodowanego kierowca odpowiada jedynie na zasadzie winy na podstawie treści art. 415 KC. W tej sytuacji bez znaczenia pozostaje okoliczność, czy w konkretnym przypadku posiadacz pojazdu równolegle ponosi odpowiedzialność na zasadzie ryzyka. Wdrożenie do polskiego ustawodawstwa obowiązkowych ubezpieczeń komunikacyjnych spowodowało, że poszkodowani sporadycznie kierują roszczenia odszkodowawcze przeciwko kierowcom. W literaturze zaznacza się, że przypisanie winy kierowcy pojazdu będącemu sprawcą wypadku jest możliwe zarówno wtedy, gdy naruszył on przepisy dotyczące bezpieczeństwa ruchu na drogach publicznych, jak i w sytuacji gdy okoliczności zaistnienia wypadku przemawiają za przypisaniem mu winy¹¹, pomimo że nie został naruszony żaden konkretny przepis.

W niektórych przypadkach kierowca pojazdu może przysługiwać roszczenie wobec posiadacza pojazdu. Punktem wyjścia oceny tych roszczeń jest art. 436 KC, który dotyczy szkód wyrządzonych m.in. pozostałym uczestnikom ruchu i nie przewiduje żadnych obostrzeń w tym zakresie. Przyjmuje się zatem, że na treść art. 436 § 1 KC może powołać się także kierowca pojazdu, jeśli jednocześnie nie jest jego posiadaczem¹². W związku z powyższym należy zarazem skonstatować, że posiadacz może niejednokrotnie zwolnić się od odpowiedzialności, dowodząc niepodzielną winę poszkodowanego będącego kierowcą. Jeżeli natomiast posiadacz nie wykaże, że szkoda nastąpiła jedynie z winy poszkodowanego, możliwe jest stosunkowe ograniczenie odszkodowania na podstawie art. 362 KC.

Odpowiedzialność z tytułu wypadku drogowego ponosi co do zasady samoistny posiadacz pojazdu mechanicznego. Przepisy prawa rzeczowego, w tym art. 336 KC, rozstrzygają o tym, kto w zaistniałej sytuacji spełnia definicję posiadacza samoistnego. Zazwyczaj jest nim właściciel pojazdu, jednak może nim być również każda osoba faktycznie władająca pojazdem w zakresie odpowiadającym treści własności¹³. Okoliczność, na jaką osobę został zarejestrowany pojazd, nie przesądza o jego własności, jednak powstaje domniemanie faktyczne co do osoby posiadacza. Natomiast z utratą posiadania mamy do czynienia przede wszystkim w sytuacji kradzieży pojazdu. Wtedy odpowiedzialność na zasadzie ryzyka ponosi złodziej, który automatycznie stał się samoistnym posiadaczem. Analogicznie sytuacja kształtuje się w stosunku do każdej osoby w sposób bezprawny używającej pojazdu. Natomiast zwolnienie posiadacza samoistnego od odpowiedzialności określonej w art. 436 § 1 KC następuje m.in. na skutek oddania pojazdu w posiadanie zależne.

Ubezpieczenie posiadacza pojazdu ponoszącego odpowiedzialność cywilną

Podstawę udzielenia ochrony ubezpieczeniowej stanowi umowa zawierana pomiędzy zakładem ubezpieczeń a ubezpieczającym. Co do zasady umowa ma charakter dobrowolny,

⁹ T. Wilms, Google Driverless Car: Why You Will Probably Never Own One, Forbes, 23.10.2013 r., <https://www.forbes.com/sites/sap/2013/10/23/google-driverless-car-why-you-will-probably-never-own-one/#2057f4f5281d> (dostęp z 25.9.2018 r.).

¹⁰ M. Matuszko, Wzrost znaczenia usług *cas sharing* impulsem dla rozwoju elektromobilności, PWC, <https://www.pwc.pl/pl/artykuly/2018/wzrost-znaczenia-uslug-car-sharing-impulsem-dla-rozwoju-elektromobilnosci.html> (dostęp z 25.9.2018 r.).

¹¹ G. Bieniek, Odpowiedzialność cywilna za wypadki drogowe, Warszawa 2007, system informacji prawnej LEX, <https://sip.lex.pl/#/monograph/369312548/7> (dostęp z 27.9.2018 r.).

¹² Por. A. Szpunar, Glosa do orzeczenia Sądu Najwyższego z 9.12.1970 r., II CR 483/70, Orzecznictwo Sądów Polskich i Komisji Arbitrażowych 1972, Nr 1, poz. 3.

¹³ Por. G. Bieniek, Odpowiedzialność... (dostęp z 27.9.2018 r.).

natomiast wyjątki od tej zasady zostały usystematyzowane w ustawie z 22.5.2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych¹⁴. Zgodnie z art. 4 pkt 1 tej ustawy ubezpieczeniem obowiązkowym w rozumieniu wskazanego aktu jest m.in. ubezpieczenie odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych za szkody powstałe w związku z ruchem tych pojazdów, tzw. ubezpieczenie OC posiadaczy pojazdów mechanicznych. Poza ubezpieczeniem obowiązkowym w stosunku do posiadaczy pojazdów mechanicznych poruszanych za pomocą sił przyrody odnosi się także dobrowolne ubezpieczenie następstw nieszczęśliwych wypadków (tzw. ubezpieczenie NW) oraz dobrowolne ubezpieczenie szkód powstałych w pojeździe i jego wyposażeniu (tzw. ubezpieczenie AC)¹⁵, które jednak ze względu na zakres niniejszego artykułu nie będą stanowiły przedmiotu jego analizy.

Obowiązkowe ubezpieczenie odpowiedzialności cywilnej (ubezpieczenie OC)

Stosownie do treści art. 436 § 1 w zw. z art. 435 KC odpowiedzialność cywilną za szkodę na osobie lub w mieniu wyrządzoną ruchem mechanicznego środka komunikacji poruszanego za pomocą sił przyrody ponosi zarówno posiadacz samoistny, jak i zależny. Natomiast art. 23 UbezObowU zobowiązuje posiadacza pojazdu mechanicznego do zawarcia umowy obowiązkowego ubezpieczenia OC za szkody powstałe w związku z ruchem posiadanego przez niego pojazdu. Powiązanie obowiązku ubezpieczenia z posiadaniem pojazdu mechanicznego znaczy tyle, że obowiązek ten obciąża zarówno posiadacza samoistnego, jak i zależnego. Ustęp 2 wskazanego przepisu rozszerza ten obowiązek m.in. na posiadacza lub kierującego pojazdem przed jego rejestracją. Zatem w pewnych przypadkach obowiązek zawarcia umowy obciąża nie tylko posiadacza, lecz również osobę kierującą pojazdem.

Ubezpieczenie odpowiedzialności cywilnej posiadacza pojazdu mechanicznego cechuje się obligatoryjnością, jednak na podstawie dyspozycji art. 3 ust. 1 UbezObowU jest to ubezpieczenie umowne, a nie ustawowe. Posiadacz pojazdu na podstawie art. 23 ust. 1 UbezObowU jest zobowiązany zawrzeć umowę obowiązkowego ubezpieczenia odpowiedzialności cywilnej. Równolegle na podstawie art. 5 ust. 2 UbezObowU obowiązek zawarcia takiej umowy obciąża także zakład ubezpieczeń posiadający zezwolenie na wykonywanie działalności ubezpieczeniowej obejmującej ubezpieczenia obowiązkowe.

Zasadniczo umowę ubezpieczenia OC zawiera się na okres 12 miesięcy, jednak art. 27 ust. 1 pkt 1–5 UbezObowU wskazuje na wyjątki, tj. kiedy istnieje możliwość zawarcia

tzw. umowy ubezpieczenia krótkoterminowego. Taki rodzaj umowy odnosi się do następujących pojazdów mechanicznych: zarejestrowanych na stałe i przeznaczonych do sprzedaży, zarejestrowanych czasowo, zarejestrowanych za granicą, będących pojazdami wolnobieżnymi, będących pojazdami historycznymi. Co do zasady posiadacz pojazdu jest zobowiązany zawrzeć umowę ubezpieczenia OC najpóźniej w dniu rejestracji pojazdu mechanicznego. Od wskazanej reguły istnieją odstępstwa, jednak nie stanowią one istotnego zagadnienia z punktu widzenia niniejszego opracowania.

Odpowiedzialność zakładu ubezpieczeń trwa przez okres wskazany w umowie i kończy się z upływem ostatniego dnia tego okresu. Treść art. 12 ust. 1 ustawy z 11.9.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej¹⁶ należy jednak skonfrontować z art. 814 § 1 KC¹⁷, który to wiąże odpowiedzialność zakładu z opłacaniem składek. Uiszczanie składek powoduje, że odpowiedzialność ubezpieczyciela wystąpi kolejnego dnia po opłaceniu składki. W przypadku umowy ubezpieczenia OC posiadacza pojazdu powyższy zapis został zawarty w treści art. 39 ust. 1 UbezObowU, stanowiąc, że odpowiedzialność zakładu ubezpieczeń rozpoczyna się z chwilą zawarcia umowy i opłacenia składki ubezpieczeniowej lub jej pierwszej raty. Jeżeli jednak w umowie wskazano późniejszy termin płatności składki, to odpowiedzialność zakładu rozpoczyna się z chwilą zawarcia umowy. Ustawa dopuszcza także możliwości odmiennego określania terminu rozpoczęcia odpowiedzialności zakładu.

Stronami umowy ubezpieczenia OC są zakład ubezpieczeń i ubezpieczający. Uprawnienie ubezpieczyciela do występowania w charakterze podmiotu stosunku ubezpieczenia zostało zdefiniowane przepisami ustawy o działalności ubezpieczeniowej i reasekuracyjnej. Zakład ubezpieczeń może wykonywać działalność ubezpieczeniową w ściśle określonej formie, przy czym wykonywanie tego typu działalności wymaga zezwolenia Komisji Nadzoru Finansowego, wobec czego jest to działalność reglamentowana.

Podstawowy obowiązek zakładu ubezpieczeń wynika z istoty umowy ubezpieczenia odpowiedzialności cywilnej (art. 822 § 1 KC), przez którą ubezpieczyciel zobowiązuje się do zapłacenia określonego w umowie odszkodowania za szkody wyrządzone osobom trzecim, wobec których odpowiedzialność za szkodę ponosi ubezpieczający albo ubezpieczony.

¹⁴ T.j. Dz.U. z 2018 r. poz. 473 ze zm.; dalej jako: UbezObowU.

¹⁵ P. Bucoń, Odpowiedzialność cywilna uczestników wypadku komunikacyjnego, Warszawa 2008, system informacji prawnej LEX, <https://sip.lex.pl/#/monograph/369182420/200758> (dostęp z 1.10.2018 r.).

¹⁶ T.j. Dz.U. z 2019 r. poz. 381 ze zm.

¹⁷ Artykuł 814 § 1 KC stanowi: Jeżeli nie umówiono się inaczej, odpowiedzialność ubezpieczyciela rozpoczyna się od dnia następującego po zawarciu umowy, nie wcześniej jednak niż od dnia następnego po zapłaceniu składki lub jej pierwszej raty.

Treść art. 34 ust. 1 i art. 35 UbezObowU ma zasadnicze znaczenie dla określenia zasad odpowiedzialności zakładu ubezpieczeń z tytułu ubezpieczenia OC posiadaczy pojazdów mechanicznych. Zgodnie z art. 34 ust. 1 UbezObowU ubezpieczenia przysługuje odszkodowanie, jeżeli posiadacz lub kierujący pojazdem mechanicznym są obowiązani do odszkodowania za wyrządzoną w związku z ruchem tego pojazdu szkodę, której następstwem jest śmierć, uszkodzenie ciała, rozstrój zdrowia bądź też utrata, zniszczenie lub uszkodzenie mienia. Natomiast na podstawie art. 35 UbezObowU ubezpieczeniem OC posiadaczy pojazdów mechanicznych jest objęta odpowiedzialność cywilna każdej osoby, która kierując pojazdem mechanicznym w okresie trwania odpowiedzialności ubezpieczeniowej, wyrządziła szkodę w związku z ruchem tego pojazdu.

Zakres przywołanych przepisów pozwala stwierdzić, że odpowiedzialność zakładu ubezpieczeń ma charakter następczy w stosunku do odpowiedzialności cywilnej posiadacza pojazdu lub kierującego pojazdem mechanicznym¹⁸. Powstaje ona w sytuacji, gdy istnieje odpowiedzialność posiadacza pojazdu bądź kierującego pojazdem na podstawie przepisów prawa cywilnego.

Możliwe sposoby obciążenia odpowiedzialnością za wypadek

Zdecydowana większość państw europejskich przyjęła koncepcję, zgodnie z którą odpowiedzialność cywilna za szkodę wynikłą z wypadku samochodowego jest niezależna od winy¹⁹. Odpowiedzialność oparta na zasadzie winy znajduje zastosowanie jedynie w niektórych systemach prawnych, w tym m.in. w Anglii, Irlandii oraz Belgii, gdzie w 1994 r. wprowadzono system automatycznej kompensacji ubezpieczeniowej, zapewniający poszkodowanemu naprawienie szkód na osobie w oderwaniu od winy sprawcy wypadku²⁰. Mając na względzie wzmożony ruch samochodowy, większość państw europejskich dokonała zaostrzenia odpowiedzialności cywilnej, opierając ją na zasadzie ryzyka.

W polskim systemie prawnym odpowiedzialność posiadacza pojazdu mechanicznego została unormowana w art. 436 KC i opiera się na zasadzie ryzyka. Powyższą zasadę wyłącza działanie siły wyższej bądź okoliczność, iż szkoda nastąpiła wyłącznie z winy poszkodowanego lub osoby trzeciej, za którą odpowiedzialności nie ponosi posiadacz pojazdu. Norma, zgodnie z którą posiadacz pojazdu mechanicznego odpowiada na zasadzie ryzyka, nie znajduje zastosowania jedynie w dwóch przypadkach. Na podstawie art. 436 § 2 zd. 1 KC w przypadku zderzenia się pojazdów mechanicznych ich posiadacze mogą żądać wzajemnie naprawienia poniesionych szkód wyłącznie na zasadach ogólnych. Natomiast zgodnie z art. 436 § 2 zd. 2 KC również tylko na zasadach ogólnych

posiadacz odpowiada za szkody wyrządzone tym, których przewozi z grzeczności.

Niezależnie od powyższego współczesna literatura w zakresie wypadków drogowych koncentruje się na dwóch ogólnych kategoriach podmiotów, które mogłyby zostać pociągnięte do odpowiedzialności za wypadki z udziałem pojazdów autonomicznych: kierujących właścicielach pojazdów bądź ich producentach²¹. Przy podejmowaniu decyzji o tym, kto powinien ponosić odpowiedzialność w sytuacji wykorzystania pojazdu w ramach *car-sharing*, możliwości zmieniają się nieznacznie. O ile w przypadku pojazdu prywatnego właścicielem i kierującym jest ta sama osoba, o tyle przy korzystaniu z samochodu w ramach systemu *car-sharing* właścicielem jest spółka wynajmująca samochód, a kierującym – „operatorem” są wszyscy pasażerowie znajdujący się w pojeździe w chwili zaistnienia wypadku²². Stwarza to trzy główne źródła osobowe przypisania odpowiedzialności: kierowcom – pasażerom, podmiotom świadczącym usługi typu *car-sharing* oraz producentom pojazdów.

1. Kierowcy – pasażerowie

W obecnym stanie prawnym odpowiedzialność za spowodowanie wypadku spoczywa w zdecydowanej mierze na kierowcach, ponieważ zazwyczaj jeden z nich, a niekiedy obaj, ponoszą winę za zaistnienie zdarzenia. Jedną z dopuszczalnych możliwości jest utrzymanie obecnego stanu rzeczy i pociąganie kierowców do odpowiedzialności za spowodowane szkody. Inny możliwym do przyjęcia wariantem znajdującym zastosowanie w systemie amerykańskim jest obarczenie odpowiedzialnością wszystkich pasażerów jadących pojazdem w chwili zaistnienia zdarzenia. W ocenie przedstawicieli doktryny amerykańskiej taka możliwość pozwala wyeliminować problemy związane z dowodzeniem faktów oraz przyjąć proste założenie, że żaden z pasażerów nie sprawuje rzeczywistej kontroli nad pojazdem. Przedstawiciele hołdujący powyższemu pogładowi wskazują, że każdy z pasażerów posiada taki sam wpływ na to, czy pojazd działa w sposób prawidłowy, wobec czego rozróżnienie na pasażerów i kierowców staje się nieuzasadnione, a wszystkie osoby poruszające się samochodem powinny być traktowane w analogiczny sposób.

¹⁸ P. Bucioń, Odpowiedzialność... (dostęp z 1.10.2018 r.).

¹⁹ Zob. T. Kadner Graziano, C. Oertel, Ein europäisches Haftungs- und Schadensrecht für Unfälle im Straßenverkehr? Eckpunkte de lege lata und Überlegungen de lege ferenda, Zeitschrift für Vergleichende Rechtswissenschaft 2008, Nr 107/2008, s. 119.

²⁰ K. Ludwiczowska, Odpowiedzialność cywilna posiadacza samochodu przy przewozie z grzeczności (zasada winy czy ryzyka), Państwo i Prawo 2009, Nr 2, s. 68–77.

²¹ Zob. G.E. Marchant, R.A. Lindor, The Coming..., s. 1321–1340.

²² C. Schroll, Splitting the Bill: Creating a National Car Insurance Fund to Pay for Accidents in Autonomous Vehicles, Northwestern University Law Review 2015, vol. 109, no. 3, s. 803–834.

Istnieje kilka metod oceny odpowiedzialności pasażerów. Po pierwsze, pasażerowie w pojeździe, który spowodował wypadek, mogliby ponosić wspólną i solidarną odpowiedzialność za wszystkie szkody powstałe w wyniku wypadku, jednak w takiej sytuacji konieczna byłaby nowelizacja przepisów Kodeksu cywilnego. Obejmowałoby to obrażenia ciała u pasażerów poruszających się samochodami biorącymi udział w wypadku oraz szkody majątkowe w tych samochodach. Alternatywnie, pasażerowie w samochodzie, który został uszkodzony, mogą pokryć wszelkie powstałe szkody, wyłączając rachunki za usługi medyczne, dotyczące pasażerów w drugim samochodzie, które mogą być opłacone z tytułu ubezpieczenia własnego. Istnieje wiele sposobów na rozłożenie szkód, przy jednoczesnym zastosowaniu zasady, że wspólną odpowiedzialność ponoszą wszyscy pasażerowie jednego z pojazdów będącego uczestnikiem zdarzenia.

Drugą możliwością jest posiadanie własnego stosownego ubezpieczenia przez wszystkich użytkowników pojazdów autonomicznych. W tym kontekście mniejsze znaczenie miałyby fakt, który z pojazdów jest winien spowodowania wypadku. W zamian za to każdy ze współpasażerów opłacałby własne koszty leczenia dzięki wykupionemu ubezpieczeniu. Ponadto pasażerowie jadący w każdym z samochodów, jak obecnie proponuje się w Stanach Zjednoczonych²³, byłiby solidarnie odpowiedzialni za szkody majątkowe powstałe w pojeździe, którym się poruszali, a jednocześnie byłiby zobowiązani pokryć odszkodowanie na rzecz podmiotu będącego właścicielem samochodu.

Analizując przedstawione powyżej możliwości, nie można także zapomnieć o wspomnianej już odpowiedzialności cywilnej posiadacza pojazdu przy tzw. przewozie z grzeczności, kiedy to posiadacz za szkody wyrządzone osobom przewożonym odpowiada na zasadach ogólnych. Rozwiązanie przyjęte przez polskiego ustawodawcę oznacza, że aby uzyskać odszkodowanie, przewożony z grzeczności poszkodowany pasażer jest zobowiązany udowodnić winę posiadacza bądź osoby, za którą ten ponosi odpowiedzialność.

W polskiej doktrynie złagodzenie odpowiedzialności posiadacza pojazdu w stosunku do pasażera przewożonego z grzeczności uzasadnia się przez odwołanie do konstrukcji działania na własne ryzyko. Koncepcja zakłada, że poszkodowany świadomie naraża się na niebezpieczeństwo²⁴, w związku z czym nie zasługuje na ochronę. obrońcy teorii podnoszą też, że trudno wymagać, aby posiadacz ponosił zaostrożoną odpowiedzialność wobec osób, którym wyświadczył uprzejmość, zatem to osoba przewożona z grzeczności powinna częściowo działać na własne ryzyko²⁵.

Zwolennicy rozwiązań, gdzie odpowiedzialność wobec pasażerów przewożonych z grzeczności opiera się na zasadzie winy, powołują się także na zasady słuszności. Podkreślają, że sprawiedliwe jest, aby ten, kto wyświadcza drugiej osobie uprzejmość, nie ponosił już surowej odpowiedzialności, a ten,

kto z grzeczności korzysta, mógł uzyskać odszkodowanie jedynie w sytuacji, gdy udowodni winę. Część przedstawicieli doktryny podnosi przy tym, że pasażer przewożony z grzeczności, w zamian za korzyści, jaki przynosi mu przewóz, w sposób milczący zrzeka się swoich uprawnień wynikających z odpowiedzialności opartej na zasadzie ryzyka²⁶. Co więcej, skoro przy przewozie z grzeczności wyłącznie przewożony odnosi korzyść, to zgodnie z zasadami słuszności tylko on powinien ponosić ryzyko tego przedsięwzięcia. Jednakże przegląd rozwiązań ustawowych przyjętych w poszczególnych krajach europejskich prowadzi do konkluzji, że obecnie złagodzenie odpowiedzialności posiadacza pojazdu mechanicznego względem pasażerów przewożonych z grzeczności stanowi rozwiązanie incydentalne²⁷.

Równolegle powinniśmy dostrzec, że istnieją wady, które odnoszą się do wszystkich wspomnianych sposobów przeniesienia odpowiedzialności na pasażerów. To natomiast tworzy system, w którym nie istnieje wina lub odpowiedzialność, ponieważ pasażerowie nie mogą przewidzieć pewnych wad, a zatem także uniknąć nieprawidłowego działania produktu²⁸. Pasażerowie nie posiadają realnego wpływu na poprawę bezpieczeństwa jadącego pojazdu, w przeciwieństwie do producentów samochodów, którzy dysponują szerokim wachlarzem możliwości pozwalającym podnosić poziom bezpieczeństwa w pojazdach. Jednak jak wskazuje część przedstawicieli amerykańskiej doktryny, producenci zostaną najbardziej zmotywowani do usprawniania systemów bezpieczeństwa, gdy staną się odpowiedzialnymi za wypadki spowodowane przez ich niebezpieczne produkty²⁹.

Koncepcja dotycząca ponoszenia odpowiedzialności przez pasażerów może jednak prowadzić do zniechęcenia części użytkowników pojazdów, którzy zdając sobie sprawę, że w sytuacji zaistnienia wypadku, staną się odpowiedzialni, w związku z czym nie będą chcieli w ogóle korzystać z systemu współdzielenia pojazdów. Można bowiem przyjąć, że całościowa odpowiedzialność pasażerów jest niewspółmierna i niesprawiedliwa, podczas gdy sukces wprowadzenia na szeroką skalę pojazdów autonomicznych zależy w dużej mierze od korzystnej dla użytkowników konstrukcji systemu prawnego. Jeśli natomiast użytkownicy zostaną zniechęceni

²³ Zob. C. Schroll, *Splitting the Bill...*, s. 803–834.

²⁴ A. Szpunar, O działaniu na własne ryzyko, *Nowe Prawo* 1978, Nr 6, s. 857.

²⁵ A. Szpunar, Odpowiedzialność za szkodę wyrządzoną osobie przewożonej z grzeczności, *Nowe Prawo* 1969, Nr 1, s. 12.

²⁶ Por. A. Rembieniński, Odpowiedzialność cywilna właściciela samochodu w stosunku do pasażera z grzeczności, *Zeszyty Naukowe Uniwersytetu Łódzkiego*, seria I, z. 35, Łódź 1964, s. 121–122.

²⁷ Zob. C. von Bar, *The Common European Law of Torts*, München 2000, s. 412 i n.

²⁸ D.M. Mele, *The Quasi-Autonomous Car as an Assistive Device for Blind Drivers: Overcoming Liability and Regulatory Barriers*, *Syracuse Journal of Science & Technology Law Reporter* 2013, vol. 28, article 2, s. 26–64.

²⁹ C. Schroll, *Splitting the Bill...*, s. 803–834.

ewentualną koniecznością ponoszenia kosztów zaistniałego wypadku, popyt na korzystanie z pojazdów autonomicznych może okazać się zbyt mały.

Na marginesie należy także zaznaczyć, że przeniesienie obowiązku ponoszenia kosztów uszkodzeń na pasażerów może dla części społeczeństwa stać w sprzeczności z założeniem, iż to producenci jako podmioty dysponujące odpowiednimi środkami pieniężnymi powinni ponosić proporcjonalną odpowiedzialność³⁰.

2. Przedsiębiorstwa stosujące system *car-sharing*

Chcąc pochylić się nad możliwą przypisania odpowiedzialności przedsiębiorstwom trudniącym się wdrażaniem systemu typu *car-sharing*, należy rozróżnić pojęcie „właściciela” pojazdu od pojęcia „operatora”. Właściciele pojazdów udostępnianych w ramach systemu, analogicznie jak w przypadku podmiotów trudniących się wypożyczaniem samochodów, stanowią kolejną potencjalną grupę osób, na którą może spaść odpowiedzialność w przypadku zaistnienia zdarzenia. Podobnie jak w przypadku kierowców, także przedsiębiorstwa mogą ponosić odpowiedzialność na różne sposoby. Podmioty mogą zostać pociągnięte do odpowiedzialności za wszelkie szkody, które wystąpiły w czasie, gdy wadliwy pojazd będący ich własnością doprowadził do zaistnienia wypadku. Natomiast w innych przypadkach przedsiębiorstwo płaciłoby jedynie za część spowodowanych uszkodzeń powstałych w samochodzie i obrażeń poniesionych przez znajdujące się w nim osoby. Sytuacja wyglądałaby analogicznie jak w przypadku przedsiębiorstw transportowych posiadających wykupione ubezpieczenia dla wszystkich pojazdów, jak też pracujących w podmiocie kierowców.

Obecnie wypożyczalnie ponoszą odpowiedzialność odszkodowawczą wobec najemców w przypadku niewykonania lub nienależytego wykonania umowy, kiedy skutek zdarzenia zawinionego przez wynajmującego najemca doznał szkody. Jeżeli okazuje się, że samochód ma wady, które ujawniły się wskutek okoliczności obciążających wynajmującego – w tym przypadku wypożyczalnię lub przedsiębiorstwo typu *car-sharing*, wynajmujący jest zobowiązany dokonać naprawy na własny koszt³¹.

Niezależnie od powyższego należy mieć na uwadze, że najemca w związku z prowadzeniem wypożyczonego pojazdu ponosi odpowiedzialność cywilną za wyrządzone przez niego szkody na mieniu i na osobie, chyba że szkoda nastąpiła wskutek siły wyższej lub wyłącznie z winy poszkodowanego lub osoby trzeciej, za które najemca nie ponosi odpowiedzialności.

Istnieje wiele powodów, ze względu na które przedsiębiorstwa trudniące się wypożyczaniem pojazdów mogą być odpowiedzialne za zaistniały wypadek. Można z dużą dozą

prawdopodobieństwa stwierdzić, że znajdują się one w lepszej sytuacji ekonomicznej niż kierowcy – pasażerowie, mogącym samym wpływać na poprawę bezpieczeństwa pojazdów autonomicznych dzięki wywieraniu presji na producentach poprzez podejmowanie odpowiednich decyzji dotyczących zakupu samochodów. Oczywiście jest, że przedsiębiorstwa prowadzące działalność typu *car-sharing*, obawiając się odpowiedzialności, będą dążyły do zakupu najbezpieczniejszych pojazdów, wymuszając na producentach stałą poprawę bezpieczeństwa produkowanych samochodów.

Ponadto, przedsiębiorstwa mają możliwość czerpania znacznych korzyści w związku z wprowadzaniem na rynek pojazdów autonomicznych, jednak równolegle stwarzając ryzyko w zakresie ich nieprawidłowego działania i możliwości spowodowania wypadku. Tego typu podmioty są skłonne podjąć ryzyko w imię zysku, zatem winny także ponosić koszty, kiedy nastąpi szkoda wynikająca z tego ryzyka. Tendencja ta jest także widoczna w innych obszarach, gdzie przedsiębiorcy czerpią zyski z tytułu podejmowanych niebezpiecznych działań.

Co więcej, w innych obszarach prawa w zakresie odnoszonych obrażeń ciała, posiadanie niebezpiecznego przedmiotu może okazać się wystarczające do przypisania odpowiedzialności w sytuacji, gdyby przedmiotem tym została spowodowana szkoda. Właściciel może podlegać karze na podstawie posiadania statusu właściciela i nie istnieje wtedy konieczność konkretyzowania działania, które spowodowało szkodę. Występuje możliwość przypisania pomiotowi odpowiedzialności deliktowej na podstawie posiadania statusu właścicielskiego.

Inną wadą związaną z przypisaniem odpowiedzialności przedsiębiorstwu jest możliwe podniesienie kosztów współużytkowania wypożyczonego pojazdu. Koszty opłacania polisy ubezpieczeniowej obejmującej wszelkie wypadki spowodowane przez pojazdy mogą okazać się na tyle wysokie, że przedsiębiorcy nie będą zainteresowani wdrożeniem autonomicznych form poruszania się na szeroką skalę. Wysokie koszty ubezpieczenia mogą także wpłynąć na niechęć tworzenia nowych podmiotów zajmujących się rozpowszechnianiem systemu *car-sharing*, co niewątpliwie spowolni wprowadzenie na rynek pojazdów autonomicznych.

3. Producenci pojazdów

Propozycja przeniesienia odpowiedzialności za wypadki spowodowane przez pojazdy autonomiczne na ich producentów uzyskała w Stanach Zjednoczonych największą liczbę

³⁰ Por. J.K. Gurney, Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles, *University of Illinois Journal of Law, Technology & Policy* 2013, vol. 2013, No. 2, s. 247–277.

³¹ Zob. Usługi wynajmu samochodów. Poradnik dla konsumentów, UOKiK, <https://uokik.gov.pl/download.php?plik=11804> (dostęp z 3.10.2018 r.).

zwolenników³². Najczęściej pojawiającym się argumentem, przemawiającym za takim sposobem pojmowania odpowiedzialności jest realny wpływ, jaki producenci posiadają na poprawę technologii, a co za tym idzie, także możliwość zredukowania skali ewentualnych zdarzeń³³. To właśnie producenci pojazdów jako podmioty zainteresowane wdrożeniem zautomatyzowanych technologii będą najprawdopodobniej ponosić winę za wypadki wywołane ruchem pojazdów autonomicznych.

Inną korzyścią może być fakt, iż w obecnym systemie istnieją ogólne ramy prawne dotyczące odpowiedzialności za produkt, które mogłyby stanowić podwaliny do stworzenia obszerniejszych i bardziej szczegółowych uregulowań. Odpowiednie zastosowanie mogłyby znaleźć przepisy Kodeksu cywilnego dotyczące odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny³⁴. Aktualnie przepisy znajdują powszechne zastosowanie w sytuacji zaistnienia szkód wyrządzonych m.in. przez wadliwy pojazd. Ponadto społeczeństwu najłatwiej byłoby zaakceptować fakt, że producenci mogą zostać pociągnięci do odpowiedzialności za wady produktu, który przecież sami stworzyli. Zatem nawet w przypadkach, w których producent nie dopuściłby się żadnego zaniedbania, opinii publicznej łatwiej byłoby przyjąć do wiadomości odpowiedzialność producenta niż kierowców – pasażerów lub przedsiębiorców wypożyczających samochody w systemie *car-sharing*.

Podobnie jak w przypadku kierowców i przedsiębiorstw zajmujących się wypożyczaniem pojazdów, pierwszym możliwym rozwiązaniem byłoby skłonienie producentów do zapłaty za wszelkie powstałe szkody. Istnieją przy tym różne sposoby podzielenia kosztów. Producent samochodu, który zawinił, mógłby pokrywać wszelkie szkody, wyłączając koszty usług medycznych własnych pasażerów, które byłyby opłacane przez ubezpieczenie własne. Zatem istnieją różne sposoby na podzielenie kosztów, przy jednoczesnym zachowaniu odpowiedzialności producenta.

Część przedstawicieli doktryny amerykańskiej stoi na stanowisku, że nałożenie odpowiedzialności na producenta jest najuczciwszym rozwiązaniem, ponieważ to właśnie wytwórca posiada najszersze spektrum możliwości, by poprawić jakość produktu i to na nim spoczywa ciężar winy za defekty zaistniałe w konstrukcji lub oprogramowaniu pojazdu na zasadzie odpowiedzialności za produkt niebezpieczny. Zgodnie bowiem z treścią art. 449¹ § 3 zd. 2 KC o tym, czy produkt jest bezpieczny, decydują okoliczności z chwili wprowadzenia go do obrotu, a zwłaszcza sposób zaprezentowania go na rynku oraz podane konsumentowi informacje o właściwościach produktu. Zatem produktem niebezpiecznym jest ten, który ma wadę stanowiącą zagrożenie dla życia i zdrowia ludzkiego, tj. samochody z wadliwym oprogramowaniem czy układem hamulcowym.

W art. 449¹ § 3 ustawodawca posługuje się tzw. kryterium „oczekiwań”, pochodzącym z reżimu rękojmi za wady,

z którego zostały wywiedzione podstawy odpowiedzialności za produkt, zwłaszcza w systemie prawnym Stanów Zjednoczonych³⁵. Jednak kryterium „oczekiwań” konsumenta ma mniejsze znaczenie w stosunkach pozaumownych, których przede wszystkim dotyczy odpowiedzialność za produkt.

W myśl art. 449¹ § 3 zd. 2 KC o tym, czy produkt jest bezpieczny, decydują okoliczności z chwili jego wprowadzenia do obrotu, sposób zaprezentowania go na rynku oraz podane informacje o właściwościach produktu. Jak wskazuje się w literaturze, o bezpieczeństwie przesądzą wszelkie okoliczności, a prezentacja produktu na rynku oraz informacje przedstawiane konsumentowi są ważne w reżimie odpowiedzialności kontraktowej. Natomiast w reżimie deliktowej odpowiedzialności za produkt kryteria te nie mają znaczenia dla poszkodowanych wadliwie niebezpiecznym produktem, np. współpasażera, przechodnia lub innego uczestnika ruchu ulicznego.

Jednocześnie producenci stale pracują nad podnoszeniem bezpieczeństwa produkowanych pojazdów tradycyjnych, a przeniesienie ciężaru na inne podmioty może doprowadzić do niebezpiecznego zjawiska zniechęcenia producentów do regularnego zwiększania poziomu bezpieczeństwa. Wszystkie wskazane okoliczności prowadzą do wniosku, że obciążenie producentów odpowiedzialnością z tytułu wypadków pojazdów autonomicznych wydaje się najbardziej racjonalną koncepcją³⁶. Nie możemy jednak zapominać, że potencjalnie wysokie koszty związane z odpowiedzialnością mogą w efekcie przełożyć się na spowolnienie prac nad wprowadzeniem do powszechnego użytku pojazdów autonomicznych³⁷.

Krajowy fundusz ubezpieczeń komunikacyjnych

Kierowcy – pasażerowie, przedsiębiorstwa świadczące usługi typu *car-sharing* oraz producenci pojazdów autonomicznych zgodnie z założeniami powinni ponosić różnego rodzaju korzyści wynikające z wprowadzenia do użytku pojazdów autonomicznych, w związku z czym nie istnieje jedno właściwe rozwiązanie pozwalające jednoznacznie określić, który z podmiotów miałby ponosić koszty będące następ-

³² M.A. Geistfeld, A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation, California Law Review 2017, vol. 105, No. 6 (12), article 2, s. 1610–1694; C. Schroll, Splitting the Bill..., s. 803–834.

³³ D.M. Mele, The Quasi-Autonomous..., s. 26–64.

³⁴ Artykuł 449¹ § 1 KC stanowi: Kto wytwarza w zakresie swojej działalności gospodarczej (producent) produkt niebezpieczny, odpowiada za szkodę wyrządzoną komukolwiek przez ten produkt.

³⁵ B. Gneta, Art. 449(1), [w:] M. Habdas, M. Fras (red.), Kodeks cywilny. Komentarz. Tom III. Zobowiązania. Część ogólna (art. 353–534), Lex/el. 2018, <https://sip.lex.pl/#/commentary/587770159/567599> (dostęp z 6.11.2018 r.).

³⁶ Zob. M. Schellekens, Self-driving cars and the chilling effect of liability law, Computer Law & Security Review 2015, vol. 31, No. 4, s. 506–517.

³⁷ Por. G.E. Marchant, R.A. Lindor, The Coming..., s. 1321–1340.

stwem wypadku. Dlatego racjonalnym wyjściem może być propozycja stworzenia krajowego funduszu ubezpieczeń komunikacyjnych, do którego mogłyby zwracać się podmioty odnoszące szkody w wyniku zdarzenia, chcąc uzyskać rekompensatę z tytułu powstałych obrażeń ciała lub uszkodzeń mienia. Analogiczne rozwiązanie zostanie niedługo wprowadzone w Stanach Zjednoczonych, gdzie obecnie z powodzeniem funkcjonują analogiczne fundusze, zapewniające finansowanie opieki medycznej lub socjalnej³⁸.

W Stanach Zjednoczonych fundusz jest finansowany ze składek opłacanych przez kierowców – pasażerów, przedsiębiorców prowadzących działalność *car-sharing* oraz producentów pojazdów, którzy wnoszą stosowne opłaty odpowiadające stopniowi korzystania z pojazdów zautomatyzowanych. Producenci wnoszą opłaty obliczane proporcjonalnie do liczby wyprodukowanych przez nich pojazdów autonomicznych w danym okresie – najczęściej roku kalendarzowym. Takie rozwiązanie znajduje uzasadnienie w tezie, zgodnie z którą im więcej samochodów stworzą producenci, a tym samym wprowadzą na drogi, tym bardziej prawdopodobne stanie się, że część z nich spowoduje wypadek.

Analogicznie przedsiębiorcy prowadzący działalność typu *car-sharing* wnoszą wkład w działanie funduszu w zależności od wielkości floty pojazdów, jaką dysponują. Oczywiście jest, że podmioty posiadające szerszą ofertę pojazdów częściej występują w roli winnego spowodowania wypadku, a zatem również często korzystają z dobrodziejstw funduszu.

Natomiast kierowcy pasażerowie opłacają składki, stosując kryterium częstotliwości korzystania z pojazdów, tak że osoby najbardziej narażone na spowodowanie wypadku opłacają składki w najwyższej wysokości.

Podmiot odpowiedzialny za dysponowanie środkami zgromadzonymi w ramach funduszu posiada uprawnienia do miarkowania wysokości składek, mogąc podnosić je kierowcom nader często powodującym wypadki, znajdującym się w grupie podwyższonego ryzyka, których utrzymanie stanowi dla funduszu największe obciążenie finansowe. W początkowej fazie wprowadzenia w życie funduszu wszyscy producenci i przedsiębiorstwa zajmujące się działalnością *car-sharing* płacą składki w tej samej wysokości. Dopiero odbiegająca od normy częstotliwość powodowania wypadków przez pojazdy należące do danego podmiotu wpływa na wzrost stawek. Opisana procedura mobilizuje producentów do stałego podnoszenia bezpieczeństwa produkowanych samochodów, a przedsiębiorstwa wypożyczające do kupowania pojazdów posiadających najlepsze właściwości z zakresu bezpieczeństwa.

W polskim systemie prawnym instytucją zajmującą się wypłatą odszkodowań i świadczeń poszkodowanym w wypadkach i kolizjach drogowych, spowodowanych przez nieubezpieczonych posiadaczy pojazdów, a także wypłatą odszkodowań osobom poszkodowanym w wypadkach dro-

gowych, gdy sprawca szkody nie został ustalony, jest Ubezpieczeniowy Fundusz Gwarancyjny (UFG)³⁹ funkcjonujący na podstawie przepisów przywołanej powyżej ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych. Według art. 98 ust. 1 tej ustawy do zadań UFG należy zaspokajanie roszczeń z tytułu ubezpieczeń obowiązkowych, tj. ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych za szkody powstałe w związku z ruchem tych pojazdów oraz ubezpieczenia odpowiedzialności cywilnej rolników z tytułu posiadania gospodarstwa rolnego⁴⁰, w granicach określonych na podstawie przepisów rozdziałów 2 i 3 ustawy, za szkody powstałe na terytorium Rzeczypospolitej Polskiej na osobie, w mieniu bądź równolegle na osobie i w mieniu.

Skoro główne zadanie UFG stanowi zaspokajanie roszczeń z tytułu ubezpieczeń obowiązkowych, to najwłaściwszym rozwiązaniem zdaje się ustawowe rozszerzenie zakresu jego działalności także na ubezpieczenia komunikacyjne pokrywające straty powstałe w wyniku wypadku spowodowanego przez pojazd autonomiczny. Ubezpieczeniowy Fundusz Gwarancyjny mógłby zajmować się zarówno zbieraniem składek odprowadzanych przez kierowców – pasażerów, producentów pojazdów oraz przedsiębiorstwa prowadzące działalność *car-sharing*, jak i wypłacaniem odszkodowań w przypadku zwrócenia się do niego przez podmioty odnoszące szkody w wyniku zdarzenia, chcące uzyskać rekompensatę z tytułu powstałych obrażeń ciała lub uszkodzeń mienia.

Podsumowanie

Stworzenie ram prawnych celem umożliwienia testowania na polskich drogach pojazdów autonomicznych poprzez wprowadzenie do polskiego systemu prawnego ustawy zmieniającej o elektromobilności i paliwach alternatywnych bez wątpienia stanowi krok w słusznym kierunku. Obecnie w związku z niezwykle szybko postępującym rozwojem nowoczesnych technologii coraz więcej państw decyduje się na udostępnianie dróg publicznych producentom pojazdów zautomatyzowanych, w celu prowadzenia na nich prac badawczych.

³⁸ Zob. D. Roos, How FICA Works, How Stuff Works, 22.2.2012, <https://money.howstuffworks.com/personal-finance/personal-income-taxes/fica.htm> (dostęp z 3.10.2018 r.).

³⁹ M. Orlicki, Ubezpieczenia obowiązkowe, Lex/el. 2011, <https://sip.lex.pl/#/monograph/369239409/4> (dostęp z 3.10.2018 r.).

⁴⁰ Zob. D. Maśniak, Art. 98, Komentarz do ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, [w:] Z. Brodecki, M. Serwach, M. Glicz (red.), Prawo ubezpieczeń gospodarczych. Tom I, Komentarz, wyd. II, Warszawa 2010, Lex/el. 2010; Z. Cwalińska-Weychert, M. Monkiewicz, G. Sordyl, Działalność odszkodowawcza Ubezpieczeniowego Funduszu Gwarancyjnego na tle rozwiązań europejskich, Prawo Asekuracyjne 2014, Nr 3(80), s. 102–116.

W związku ze stopniowym pojawianiem się na drogach coraz większej ilości pojazdów autonomicznych ogólna liczba wypadków drogowych powinna zmaleć. Należy jednak zwrócić uwagę, że zaistniałe zdarzenia przybiorą zgoła odmienny od dotychczasowych charakter, w związku z czym obecnie funkcjonujący system odpowiedzialności cywilnej oparty w głównej mierze na obowiązkowym ubezpieczeniu OC posiadaczy pojazdów mechanicznych za szkody powstałe w związku z ruchem tych pojazdów może okazać się niewystarczający.

Tymczasem przedstawiciele doktryny wymieniają trzy podstawowe kategorie podmiotów, które mogłyby zostać pociągnięte do odpowiedzialności za spowodowanie wypadku z udziałem pojazdu autonomicznego: kierowców – pasażerów, podmioty świadczące usługi typu *car-sharing* oraz producentów pojazdów. Najbardziej racjonalną koncepcją zdaje się jednak być nałożenie odpowiedzialności na producenta posiadającego najszersze spektrum możliwości, by podnosić jakość produktu. To właśnie na wytwórcy spoczywa ewentualny ciężar winy w związku z wadami zaistniałymi w konstrukcji lub oprogramowaniu pojazdu. Pasażerowie nie mają bowiem realnego wpływu na poprawę bezpieczeństwa jadącego pojazdu, w przeciwieństwie do producentów samochodów. Kontrowersyjna teoria zakłada, że producenci zostaną najbardziej zmotywowani do usprawniania systemów

bezpieczeństwa, gdy staną się odpowiedzialnymi za wypadki spowodowane przez ich niebezpieczne produkty. Tym samym na producencie spoczywa ciężar winy za defekty zaistniałe w konstrukcji lub oprogramowaniu pojazdu na zasadzie odpowiedzialności za produkt niebezpieczny. Do produktów niebezpiecznych w kontekście pojazdów autonomicznych należy zaliczyć np. samochody z wadliwym oprogramowaniem bądź układem hamulcowym.

Innym korzystnym rozwiązaniem może być zaczerpnięta z ustawodawstwa amerykańskiego propozycja stworzenia krajowego funduszu ubezpieczeń komunikacyjnych, finansowanego ze składek opłacanych przez kierowców – pasażerów, przedsiębiorstwa prowadzące działalność typu *car-sharing* oraz producentów pojazdów, wnoszących stosowne opłaty odpowiadające stopniowi ich korzystania z pojazdów zautomatyzowanych.

Biorąc pod uwagę, że większość znaczących koncernów samochodowych w perspektywie najbliższych lat zamierza wprowadzić do swojej oferty w pełni zautomatyzowane pojazdy, ustawodawca powinien pochylić się nad problematyką zaprezentowaną w niniejszym artykule, uszczegóławiając uregulowania odnoszące się m.in. do odpowiedzialności za produkt niebezpieczny czy odpowiedzialności ponoszonej przez posiadacza pojazdu przewożącego pasażerów z grzeczności.

Słowa kluczowe: pojazd autonomiczny, odpowiedzialność, fundusz ubezpieczeń komunikacyjnych.

The possibility to hold an entity liable for an accident of an autonomous vehicle and the concept of creating a national car insurance fund as a form of reimbursement of costs

The subject of this article is the analysis of the possibility of creating a national car insurance fund financed from contributions paid by entities using autonomous vehicles. Simultaneously, the fund would be a form of reimbursement of costs, and people who suffered damage as a result of an incident, in order to obtain compensation for the injury or property damage, could turn directly to the fund. At the same time, the author presents possibilities of holding individual entities liable at civil law for the damage resulting from a car accident caused by an autonomous vehicle.

Keywords: autonomous vehicle, civil liability, car insurance fund.



beck.pl
Wydawnictwo C.H. BECK



www.beck.pl

Doręczenia elektroniczne pomiędzy podmiotami publicznymi w postępowaniu

r.pr. Sylwester Szczepaniak¹

W niniejszej glosie autor omawia dwa postanowienia NSA dotyczące doręczeń elektronicznych pomiędzy podmiotami publicznymi w postępowaniu, do którego zastosowanie znajdują przepisy Kodeksu postępowania administracyjnego. Naczelny Sąd Administracyjny w tych orzeczeniach uznał, że za dzień doręczenia aktu administracyjnego organowi publicznemu uznaje się dzień potwierdzenia odbioru przez złożenie podpisu elektronicznego przez pracownika urzędu, a nie dzień wystawienia poświadczenia przedłożenia wystawionego przez elektroniczną skrzynkę podawczą. W glosie opisano oba orzeczenia z uwagi na podobny stan faktyczny oraz podobne wnioski. Ważnym argumentem był też fakt, iż głosowane orzeczenia są stosunkowo nowe. Glosa ma charakter krytyczny w stosunku do przedstawionych przez NSA wniosków. W ocenie autora glosy zapadłe orzeczenia nie uwzględniają specyfiki podmiotów publicznych – nawet jeżeli występują one jako strona w postępowaniu administracyjnym oraz przepisów ustawy z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne².

Uwagi wstępne

Glosa odnosi się do dwóch nowych orzeczeń NSA, tj. do postanowienia z 16.1.2018 r.³ oraz z 23.3.2018 r.⁴. W obu orzeczeniach, zapadłych w odrębnych stanach faktycznych, kluczowym zagadnieniem prawnym była ocena, czy pismo organu doręczone na elektroniczną skrzynkę podawczą faktycznie zostało doręczone do strony postępowania będącej jednocześnie podmiotem publicznym, tj. gminą, w sposób prawidłowy oraz – w przypadku uznania za doręczenie prawidłowe – od którego dnia rozpoczął biec termin dla tego podmiotu publicznego (strony) na dokonanie czynności. Sądy oceniały, czy termin ten biegnie od dnia wniesienia pisma na elektroniczną skrzynkę podawczą – strony (podmiotu publicznego w rozumieniu ustawy o informatyzacji), tj. od dnia otrzymania Urzędowego Poświadczenia Przedłożenia czy też od dnia potwierdzenia odebrania otrzymania Urzędowego Poświadczenia Doręczenia.

Postanowienie NSA z 23.3.2018 r. – stan faktyczny

Gmina Byczyna brała udział w konkursie organizowanym przez Ministra Kultury i Dziedzictwa Narodowego w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014–2020. Celem gminy było zdobycie dofinansowania na realizację projektu z udziałem budżetu UE. Gmina Byczyna 22.12.2017 r. otrzymała informację Ministra Rozwoju i Finansów, wydaną w tym samym dniu, tj. 22.12.2017 r. (czego dowód stanowi urzędowe poświadczenie odbioru nadesłane przez organ). Następnie 9.1.2018 r. Gmina Byczyna złożyła skargę do WSA w Warszawie w przedmiocie oceny złożonego przez nią wniosku. Wojewódzki Sąd Administracyjny

postanowieniem pozostawił skargę bez rozpatrzenia. Uzasadniając, WSA wskazał, że postępowanie sądowoadministracyjne wszczęte skargami dopuszczalnymi przez ustawę z 11.7.2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014–2020⁵ realizowane jest w sposób odmienny niż przewiduje to ustawa z 30.8.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi⁶. W związku z tym, zgodnie z art. 61 ust. 2 ustawy wdrożeniowej, skarga wnoszona jest przez wnioskodawcę w terminie 14 dni od dnia otrzymania informacji bądź w terminie 14 dni od dnia upływu terminu na uzupełnienie protestu lub poprawienie w nim oczywistych omyłek, bezpośrednio do właściwego wojewódzkiego sądu administracyjnego wraz z kompletną dokumentacją w sprawie. Natomiast wniesienie skargi po tym terminie skutkuje pozostawieniem jej bez rozpatrzenia. Sąd I instancji, biorąc powyższe pod uwagę, stwierdził, że urzędowe poświadczenie przedłożenia stanowi o skutecznym doręczeniu rozstrzygnięcia stronie skarżącej 22.12.2017 r. natomiast wniesienie skargi dopiero 9.1.2018 r. uznane pozostaje za wniesione po terminie. W związku z tym sąd I instancji pozostawił skargę bez rozpatrzenia.

Gmina złożyła skargę kasacyjną, wskazując naruszenie:

- art. 61 ust. 6 pkt 1 ustawy wdrożeniowej (poprzez uznanie, że skarga została wniesiona po terminie);

¹ Autor jest asystentem w Zakładzie Prawa Administracyjnego w Instytucie Nauk Prawnych Polskiej Akademii Nauk. Pracownik administracji rządowej. Zajmuje się prawem administracyjnym, w tym prawem samorządu terytorialnego oraz zagadnieniami prawa nowych technologii w administracji publicznej.

² T.j. Dz.U. z 2019 r. poz. 700 ze zm.; dalej jako: InfPodPubU.

³ II OZ 1649/17, Legalis.

⁴ I GSK 157/18, Legalis.

⁵ T.j. Dz.U. z 2017 r. poz. 1460 ze zm.; dalej jako: ustawa wdrożeniowa.

⁶ T.j. Dz.U. z 2018 r. poz. 1302 ze zm.; dalej jako: PrPosSądAminU.

– art. 46 § 4 pkt 3 KPA w zw. z art. 20a InfPodPubU, a także w zw. z § 11 ust. 1 pkt 1 i ust. 2 pkt 2, § 14, 15 i 16 rozporządzenia Prezesa Rady Ministrów z 14.9.2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych⁷ oraz art. 46 § 5 i 6 KPA (poprzez bezzasadne uznanie, że gmina otrzymała zaskarżoną informację 22.12.2017 r., podczas gdy na podstawie powyższych przepisów za dzień doręczenia powinno się uznać 27.12.2017 r.).

Naczelny Sąd Administracyjny uznał skargę za zasadną. Odnosząc się do zarzutu naruszenia przez sąd I instancji art. 61 ust. 6 pkt 1 ustawy wdrożeniowej, NSA wskazał, że sąd I instancji nie wyjaśnił w dostateczny sposób w uzasadnieniu zaskarżonego postanowienia, kiedy doręczenie jest skuteczne w przypadku doręczania pisma za pomocą środków komunikacji elektronicznej. Naczelny Sąd Administracyjny zwrócił również uwagę, że art. 67 ustawy wdrożeniowej stanowi, że do procedury odwoławczej nie stosuje się przepisów Kodeksu postępowania administracyjnego, z wyjątkiem wyłączenia pracowników organu, doręczeń i sposobu obliczania terminów. Odnosząc się zaś do drugiego z zarzutów, NSA zauważył, że zgodnie z art. 46 § 1 KPA odbierający pismo potwierdza doręczenie mu pisma swoim podpisem ze wskazaniem daty doręczenia. Artykuł 46 § 3 KPA wskazuje natomiast, że w przypadku doręczenia pisma za pomocą środków komunikacji elektronicznej doręczenie jest skuteczne, jeżeli adresat potwierdzi odbiór pisma w określony w § 4 pkt 3 sposób. Organ administracji publicznej ma bowiem obowiązek przesłać temu adresatowi zawiadomienie zawierające pouczenie dotyczące sposobu odbioru pisma. Sposób podpisania tego rodzaju dokumentu został określony w art. 20 InfPodPubU. Sąd wskazał, że ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne określa zasady wymiany informacji drogą elektroniczną, w tym dokumentów pomiędzy podmiotami publicznymi. Powyższa ustawa wraz z wydanym na jej podstawie rozporządzeniem w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych określa zasady doręczania dokumentów elektronicznych za pośrednictwem platformy e-PUAP. Zgodnie z art. 3 pkt 20 InfPodPubU urzędowe poświadczenie odbioru to dane elektroniczne powiązane z dokumentem elektronicznym doręczonym podmiotowi publicznemu lub przez niego doręczanym w sposób zapewniający rozpoznawalność późniejszych zmian dokonanych w tych danych. Urzędowe poświadczenie przedłożenia (UPP) oraz urzędowe poświadczenie doręczenia (UPD) zostały zdefiniowane w rozporządzeniu Prezesa Rady Ministrów z 14.9.2011 r. Zgodnie z § 11 ust. 1 pkt 1 ww. rozporządzenia doręczenie dokumentu elektronicznego na informatycznym nośniku danych może być potwierdzone poświadczeniem przedłożenia (UPP), które jest przesyłane na

adres poczty elektronicznej. W przypadku odebrania dokumentu elektronicznego przez elektroniczną skrynkę podawczą podmiotu publicznego poświadczenie przedłożenia jest automatycznie tworzone i udostępniane nadawcy tego dokumentu. Automatyczne wygenerowanie przez system UPP pozwala przyjąć, że dokument wpłynął do urzędu. Natomiast zgodnie z § 14, 15 i 16 tego rozporządzenia proces tworzenia urzędowego poświadczenia doręczenia (UPD) wygląda inaczej. W tym przypadku doręczenie wymaga świadomego przyjęcia przesyłki przez adresata i dokonania potwierdzenia odbioru przez złożenie podpisu elektronicznego. Dopiero po weryfikacji podpisu elektronicznego system teleinformatyczny udostępnia adresatowi do pobrania doręczany dokument elektroniczny wraz z podpisanym przez niego poświadczeniem doręczenia oraz udostępnia organowi doręczającemu podpisane poświadczenie doręczenia.

Sąd zauważył, że skarżąca (gmina) jest także podmiotem publicznym, co może być przyczyną wątpliwości przy wydawaniu rozstrzygnięcia. Jednakże w przedstawionej sytuacji, w ocenie NSA, gmina występuje jako strona postępowania nadzorczego oraz jako strona skarżąca w postępowaniu sądowoadministracyjnym. Dlatego też musi dojść do doręczenia dokumentu przesłanego drogą elektroniczną, a nie tylko jego przedłożenia w systemie teleinformatycznym podmiotu publicznego będącego jednocześnie stroną postępowania. Dopiero bowiem po potwierdzeniu odebrania dokumentu elektronicznego przez potwierdzenie poświadczenia doręczenia podpisem elektronicznym dokument ten udostępnia się adresatowi. Oznacza to, że za datę doręczenia dokumentu elektronicznego należało uznać datę opatrzenia poświadczenia doręczenia podpisem elektronicznym.

Postanowienie NSA z 16.1.2018 r. – stan faktyczny

Wojewódzki Sąd Administracyjny w Szczecinie odmówił Powiatowi Myśliborskiemu przywrócenia terminu do wniesienia skargi na rozstrzygnięcie nadzorcze Wojewody Zachodniopomorskiego z 16.8.2017 r. w przedmiocie stwierdzenia nieważności uchwały w sprawie zmiany okresu piastowania stanowiska Dyrektora Centrum Usług Wspólnych Powiatu Myśliborskiego. Rozstrzygnięcie nadzorcze stwierdzało nieważność uchwały Zarządu Powiatu w Myśliborzu z 12.4.2017 r. Rozstrzygnięcie nadzorcze zostało doręczone skarżącemu z wykorzystaniem poczty elektronicznej (ePUAP) 25.8.2017 r., o czym świadczy poświadczenie przedłożenia w aktach administracyjnych. Powiat Myśliborski 26.9.2017 r. zaskarżył do Wojewódzkiego Sądu Administracyjnego rozstrzygnięcie nadzorcze Wojewody Zachodniopomorskiego,

⁷ T.j. Dz.U. z 2018 r. poz. 180 ze zm.

jednocześnie wnosząc o przywrócenie terminu do złożenia skargi. Za uzasadnienie uznał fakt, że uchybienie terminu nie nastąpiło z jego winy i było wynikiem błędu pracownika biura obsługi klienta Starostwa Powiatowego w Mysliborzu. Rozstrzygnięcie nadzorcze zostało bowiem przesłane przez organ drogą elektroniczną (platformą e-PUAP) 25.8.2017 r. o godzinie, o której starostwo powiatowe już nie pracowało. Pracownik owego starostwa uznał więc za nieskuteczne doręczenie pisma po godzinach urzędowania i za dzień doręczenia rozstrzygnięcia nadzorczego przyjął kolejny następujący dzień, w którym to starostwo świadczyło pracę. Skarżący wyjaśnił, że dopiero kancelaria prawna po dokładnej analizie przepisów dotyczących elektronicznego systemu doręczeńowego uznała, że w zaistniałej sytuacji właściwą datą doręczenia kopii rozstrzygnięcia nadzorczego jest data 25.8.2017 r. Wojewódzki Sąd Administracyjny odmówił przywrócenia terminu. Wskazał bowiem, że błąd pracownika polegający na wadliwym przyporządkowaniu wpływu korespondencji świadczy o niedołożeniu należytej staranności. I w takiej sytuacji winę powinien ponieść pracodawca, ponieważ to na nim ciąży obowiązek przeszkolenia swoich pracowników w zakresie prawidłowego odbioru i oznaczania korespondencji przy wykorzystaniu systemu ePUAP. Gmina wniosła zażalenie na powyższe postanowienie, powołując się na naruszenie:

- art. 86 § 1 PrPosSądAminU (poprzez nieuzasadnioną odmowę przywrócenia terminu);
- art. 88 PrPosSądAminU oraz art. 109 w zw. z art. 391 § 1 KPA i w zw. z art. 79 ust. 5 ustawy z 5.6.1998 r. o samorządzie powiatowym⁸ oraz art. 3 pkt 2, art. 20b ust. 2 InfPodPubU – w ocenie gminy bowiem nie doszło do uchybienia terminu do wniesienia skargi, ponieważ Wojewoda Zachodniopomorski nie doręczył skarżącemu rozstrzygnięcia nadzorczego w rozumieniu przepisów ustawy o samorządzie powiatowym, a jedynie nieopatrzoną podpisem elektronicznym kopię tego rozstrzygnięcia. W rozumieniu zaś ustawy o informatyzacji dokument taki nie stanowi dokumentu elektronicznego.

Naczelny Sąd Administracyjny uznał, że zażalenie zasługuje na uwzględnienie, jednakże z innych przyczyn niż podniesione przez skarżącego. Sąd ten zauważył, że postępowanie nadzorcze nie jest administracyjnym postępowaniem jurysdykcyjnym, rozstrzygnięcie zaś nadzorcze nie jest decyzją administracyjną w związku, z tym stosowanie Kodeksu postępowania administracyjnego ma wyłącznie charakter pomocniczy. Zgodnie z art. 46 § 1 KPA odbierający pismo potwierdza doręczenie mu pisma swoim podpisem ze wskazaniem daty doręczenia. Artykuł 46 § 3 KPA wskazuje natomiast, że w przypadku doręczenia pisma za pomocą środków komunikacji elektronicznej doręczenie jest skuteczne, jeżeli adresat potwierdzi odbiór pisma w określony w § 4 pkt 3 sposób. Organ administracji publicznej ma bowiem obowiązek

przesłać adresatowi zawiadomienie zawierające pouczenie dotyczące sposobu odbioru pisma. Sposób podpisania tego rodzaju dokumentu został określony w art. 20 InfPodPubU. W danej sprawie rozstrzygnięcie nadzorcze zostało przesłane w formie elektronicznej, potwierdzenie zaś przesłania zostało wygenerowane przez system poświadczeniem przedłożenia (UPP) z 25.8.2017 r. Natomiast w aktach sprawy brak jest urzędowego potwierdzenia doręczenia (UPD) opatrzonego podpisem elektronicznym, umożliwiającego identyfikację. Biorąc powyższe pod uwagę, NSA stwierdził, że sąd I instancji nie miał możliwości oceny, czy skarga została wniesiona w terminie, wskazana bowiem na dokumencie UPP data doręczenia jest wyłącznie datą doręczenia tego poświadczenia nadawcy, a więc datą, w której Wojewoda Zachodniopomorski otrzymał w dokumencie UPP wygenerowany automatycznie przez system teleinformatyczny skarżącego. Nie można uznać jednak, że jest to data doręczenia rozstrzygnięcia nadzorczego.

Zdaniem glosatora

Tezy zawarte w orzeczeniach NSA dotyczące doręczenia elektronicznego za pomocą elektronicznej skrzynki podawczej należy poddać krytyce. Należy wskazać, że norma z art. 39¹ KPA wprowadzająca możliwość stosowania doręczeń elektronicznych została dodana do na mocy art. 36 pkt 1 InfPodPubU. Następnie regulacja Kodeksu postępowania administracyjnego była kilkakrotnie zmieniana przez kolejne ustawy. Artykuł 39¹ KPA wyznacza ramy doręczania stronom i innym uczestnikom postępowania pism w formie dokumentów elektronicznych w toku postępowania. W wyniku wejścia w życie ustawy z 7.4.2017 r. o zmianie ustawy Kodeks postępowania administracyjnego oraz niektórych innych ustaw⁹ po art. 39¹ KPA dodano art. 39² KPA, który to przepis wyznacza ramy doręczania dokumentów elektronicznych podmiotowi publicznemu, w przypadku gdy jest on stroną lub innym uczestnikiem postępowania i jest obowiązany do udostępniania i obsługi elektronicznej skrzynki podawczej na podstawie art. 16 ust. 1a InfPodPubU. Zgodnie z tym przepisem, w przypadku gdy stroną lub innym uczestnikiem postępowania jest podmiot publiczny obowiązany do udostępniania i obsługi elektronicznej skrzynki podawczej na podstawie art. 16 ust. 1a InfPodPubU doręczenia dokonuje się na elektroniczną skrzynkę podawczą tego podmiotu. Artykułu 39¹ się nie stosuje. Jak wskazuje uzasadnienie do projektu tej ustawy (druk sejmowy Nr 1183), celem wprowadzenia tego przepisu było wyrażenie wprost zasady, że do podmiotu publicznego nie będą stosowane przepisy Kodeksu postępowania administracyjnego doty-

⁸ T.j. Dz.U. z 2019 r. poz. 511 ze zm.

⁹ Dz.U. poz. 935.

czące wymogu uzyskania uprzedniej zgody na doręczanie pism w trybie opisanym w art. 39¹ KPA. Szczegółowe zasady doręczania pism w postępowaniu administracyjnym zostały określone w art. 46 KPA. Uregulowania zawarte w art. 46 § 1–2 dotyczą zasad doręczania pism w formie tradycyjnej, a art. 46 § 3–10 pism doręczania pism w formie dokumentu elektronicznego. Na tle tych przepisów wyróżnia się art. 46 § 10 stanowiący: „Doręczenie pisma w formie dokumentu elektronicznego do podmiotu publicznego w rozumieniu przepisów ustawy, o której mowa w § 4 pkt 3, następuje przez elektroniczną skrzynkę podawczą tego podmiotu, w sposób określony w tej ustawie”. Przepis ten został dodany do na mocy ustawy z 12.2.2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw¹⁰, przy czym pierwotnie był on oznaczony jako ust. 6. Nowe, w stosunku do poprzedniego brzmienia przepisu, było postanowienie art. 46 § 4 pkt 3 KPA w brzmieniu: „W celu doręczenia dokumentu w formie dokumentu elektronicznego organ administracji publicznej, z zastrzeżeniem § 6, przesyła na adres elektroniczny adresata informację zawierającą: pouczenie dotyczące sposobu odbioru dokumentu, a w szczególności sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym organu administracji publicznej oraz informacji o wymogu podpisania urzędowego poświadczenia odbioru w sposób wskazany w art. 20a InfPodPubU”. Przepis w podobnym brzmieniu, tj. ze sformułowaniem „z zastrzeżeniem § 6”, obowiązywał do 11.5.2014 r., czyli do dnia wejścia w życie ustawy z 10.1.2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw¹¹. Ustawodawca, rezygnując z tego zastrzeżenia, nie wyjaśnił w uzasadnieniu do projektu tej ustawy (druk sejmowy Nr 1637) przyczyn podjętego rozwiązania. Ta niewielka zmiana natury konstrukcyjnej nie zmienia interpretacji tego przepisu. Otóż art. 46 § 10 KPA jest przepisem szczególnym w stosunku do przepisów art. 46 § 3–9, tzn. postanowienia § 3–9 nie mają zastosowania do sytuacji uregulowanej w § 10 tego przepisu. Faktem jest, że przywołany art. 46 § 4 pkt 3 KPA nie wskazuje żadnej ustawy, niemniej jednak nie rodzi wątpliwości, że zamierzeniem ustawodawcy było odwołanie się do ustawy o informatyzacji. Artykuł 46 § 4 pkt 3 KPA w brzmieniu sprzed nowelizacji, która weszła w życie w 10.6.2017 r., powoływał się właśnie na tę ustawę. Takie stanowisko prezentuje także NSA w postanowieniu z 23.3.2018 r.¹².

Szczególnie istotny z punktu widzenia oceny głosowanych orzeczeń jest art. 3 pkt 20 InfPodPubU. Przepis ten zawiera bowiem definicję urzędowego poświadczenia odbioru. Zgodnie z nią przez urzędowe poświadczenie odbioru rozumie się „dane elektroniczne powiązane z dokumentem elektronicznym doręczonym podmiotowi publicznemu lub przez

niego doręczanym w sposób zapewniający rozpoznawalność późniejszych zmian dokonanych w tych danych, określające:

- a) pełną nazwę podmiotu publicznego, któremu doręczono dokument elektroniczny lub który doręcza dokument,
- b) datę i godzinę wprowadzenia albo przeniesienia dokumentu elektronicznego do systemu teleinformatycznego podmiotu publicznego – w odniesieniu do dokumentu doręczanego podmiotowi publicznemu,
- c) datę i godzinę podpisania urzędowego poświadczenia odbioru przez adresata z użyciem mechanizmów, o których mowa w art. 20a ust. 1 albo 2 – w odniesieniu do dokumentu doręczanego przez podmiot publiczny,
- d) datę i godzinę wytworzenia urzędowego poświadczenia odbioru”.

Zdefiniowane wyżej urzędowe poświadczenie odbioru jest określeniem wspólnym dla urzędowego poświadczenia przedłożenia (czyli UPP), do którego odnosi się art. 3 pkt 20 lit. b) InfPodPubU, i urzędowego poświadczenia doręczenia (czyli UPD), do którego odnosi się art. 3 pkt 20 lit. c) InfPodPubU. Zasady tworzenia UPP i UPD określone zostały w rozporządzeniu w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych. Stosownie do § 13 ust. 1 tego rozporządzenia w przypadku odebrania dokumentu elektronicznego przez elektroniczną skrzynkę podawczą podmiotu publicznego poświadczenie przedłożenia jest automatycznie tworzone i udostępniane nadawcy tego dokumentu przez system teleinformatyczny służący do obsługi doręczeń. Zgodnie zatem z brzmieniem przywołanego przepisu UPP generowane jest w sytuacji, gdy dany dokument elektroniczny został odebrany przez system teleinformatyczny podmiotu publicznego, a inaczej rzecz ujmując – doręczony do podmiotu publicznego. W praktyce oznacza to, że jeżeli dana osoba wniosła podanie drogą elektroniczną do podmiotu publicznego, zgodnie z warunkami korzystania z platformy e-PUAP, to automatyczne wygenerowanie UPP pozwala jej przyjąć, że dokument ten wpłynął do urzędu. Urzędowe potwierdzenie przedłożenia stanowi zatem pewnego rodzaju kompilację papierowego „potwierdzenia nadania” oraz papierowego „potwierdzenia odbioru”, a w konsekwencji należy wiązać z nim takie skutki prawne, jakie Kodeks lub inny akt prawny wiąże z odebraniem dokumentu przez podmiot publiczny działający czy to jako organ administracji publicznej, czy to jako strona lub uczestnik postępowania administracyjnego. Poświadczenie przedłożenia generowane jest przez system teleinformatyczny podmiotu publicznego w sytuacji odebrania dokumentu elektronicznego, co jest możliwe z uwagi

¹⁰ Dz.U. Nr 40, poz. 230.

¹¹ Dz.U. poz. 183.

¹² I GSK 157/18, Legalis.

na to, że na podmioty publiczne został nałożony obowiązek posiadania systemu teleinformatycznego, który posiada określone funkcjonalności, a odnosząc to do zagadnienia będącego przedmiotem niniejszego wywodu – daje gwarancję, że UPP tworzone jest w przypadku odebrania dokumentu przez system teleinformatyczny danego podmiotu publicznego. Niewątpliwie owa funkcjonalność systemu teleinformatycznego zapewnia automatyzację czynności, które w systemie korespondencji papierowej były związane z wypełnieniem druku potwierdzenia nadania i druku potwierdzenia odbioru. Informatyzacja administracji publicznej nie tylko przyspiesza proces w zakresie doręczeń dokonywanych wewnątrz administracji, ale także skutkuje zmniejszeniem zaangażowania pracowników podmiotów publicznych. Okoliczność rozdzielania urzędowego potwierdzenia odbioru na urzędowe potwierdzenie przedłożenia i urzędowe potwierdzenie odbioru podyktowana była nie tylko charakterem strony lub uczestnika postępowania, tj. bycia podmiotem publicznym lub innym podmiotem, ale także kwestiami organizacyjnymi. O ile bowiem podmioty publiczne zostały zobowiązane do posiadania systemu teleinformatycznego, który daje gwarancję, o jakiej była mowa powyżej, o tyle na inne podmioty, a więc w szczególności osoby fizyczne, takiego obowiązku nie można było nałożyć. A zatem skoro podmioty inne niż podmioty publiczne nie posiadają systemu umożliwiającego w sposób niezaprzeczalny generowanie informacji potwierdzającej odebranie dokumentu elektronicznego i systemu, który jest kompatybilny z systemem teleinformatycznym podmiotów publicznych, to w konsekwencji należało w ramach systemu teleinformatycznego podmiotu publicznego utworzyć platformę doręczeńową. Stąd też UPD ma zastosowanie do innych podmiotów niż podmioty publiczne, a cały proces jego uzyskiwania został opisany w art. 46 § 3–99 KPA oraz § 14 rozporządzenia, o którym mowa powyżej. System ePUAP aktualnie nie daje możliwości stosowania UPD względem podmiotów publicznych czy też zawiadomień, o jakich mowa w art. 46 § 4 KPA, co jest wynikiem stosowania przepisów tego kodeksu w zakresie doręczeń korespondencji drogą elektroniczną do podmiotów publicznych. Odnosząc się do zagadnienia w przedmiocie tego, czy w wyniku przekazania przez jeden podmiot publiczny, np. organ administracji, korespondencji do innego podmiotu publicznego na jego ESP możliwe jest uwierzytelnienie odbiorcy zgodnie z zasadami określonymi w art. 20a InfPodPubU lub w inny sposób umożliwiający złożenie podpisu na UPD, wyjaśniam, że dostępem do elektronicznej skrzynki podawczej na ePUAP zarządza administrator danego podmiotu. Podmioty, którym Minister Cyfryzacji nadał funkcjonalność podmiotu publicznego, zostają wcześniej weryfikowane zgodnie z rozporządzeniem Ministra Cyfryzacji z 5.10.2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej¹³. Jeśli chodzi o możliwość

zidentyfikowania osoby, która odebrała czy otworzyła dany dokument, to warto mieć na względzie, że dostępem do konta zarządza administrator danego podmiotu, co oznacza, że to administrator nadaje dostęp do składu konkretnej osobie po uprzednim wskazaniu przez nią jej identyfikacji w systemie ePUAP.

Z powyższego wynika, że wolą ustawodawcy jest, aby na gruncie przepisów Kodeksu postępowania administracyjnego nie traktować podmiotu publicznego występującego w postępowaniu administracyjnym jak każdej innej strony postępowania (osoby fizycznej, podmiotu prywatnego itp.) z uwagi na różnice wprowadzone art. 39² KPA. W szczególności za takim stanowiskiem przemawia ostatnia nowelizacja Kodeksu postępowania administracyjnego, która weszła w życie 27.6.2017 r. Zgodnie z wprowadzonym na gruncie ww. nowelizacji art. 39² KPA, w przypadku gdy stroną lub innym uczestnikiem postępowania jest podmiot publiczny obowiązany do udostępniania i obsługi elektronicznej skrzynki podawczej na podstawie art. 16 ust. 1a InfPodPubU doręczenia dokonuje się na elektroniczną skrzynkę podawczą tego podmiotu. Artykułu 39¹ w tym przypadku się nie stosuje. Artykuł 39² KPA ma więc charakter wyjątku i jako taki musi być rozumiany przy stosowaniu wykładni ścisłej. Jednakże w swojej aksjologii wskazuje on na zróżnicowanie sytuacji podmiotu publicznego, który może być stroną postępowania administracyjnego od innej strony. Do podmiotu publicznego stosuje się inny standard doręczeń związany z faktem, że na podstawie przepisów ustawy o informatyzacji posiada on Elektroniczną Skrzynkę Podawczą, a przepisy w sposób dookreślony wskazują sposób komunikacji podmiotów publicznych za pomocą ww. skrzynki. Należy więc dokonywać takiej wykładni Kodeksu postępowania administracyjnego, która jest zsynchronizowana z ustawą o informatyzacji podmiotów realizujących zadania publiczne. Jest to wykładnia systemowa opierająca się na założeniu, że system prawa jest niesprzeczny i zupełny. Oczywiście pojawia się pytanie, czy takie zróżnicowanie jest zgodne z Konstytucją RP, która w art. 32 KPA wskazuje jednoznacznie, że wszyscy są wobec prawa równi. Wszyscy mają prawo do równego traktowania przez władze publiczne. Następnie dodaje, że nikt nie może być dyskryminowany w życiu politycznym, społecznym lub gospodarczym z jakiejkolwiek przyczyny. Bogate orzecznictwo TK, którego z uwagi na objętość glosy nie będę przytaczał, ograniczając się jedynie do wskazania dominującego stanowiska, wskazuje, że zasada równości nie ma waloru absolutnego oraz musi być rozważana wyłącznie w przypadku podmiotów posiadających te same cechy. W ocenie autora niniejszej glosy, mając na uwadze powyższe wskazania TK, należy uznać, że w przypadku podmiotów

¹³ Dz.U. poz. 1626.

publicznych nie znajduje zastosowania zasada równości. Nie można bowiem strony – która jest podmiotem prywatnym (osoby fizycznej, osoby prawnej i jednostki organizacyjnej nieposiadającej osobowości prawnej, którym ustawa przyznaje zdolność prawną) porównywać z podmiotem publicznym – który działa na podstawie przepisów prawa i realizuje zadania publiczne, mimo że obie przedstawione kategorie podmiotów są stronami – w rozumieniu przepisów Kodeksu postępowania administracyjnego. Gwarancje procesowe (takie jak zasada oficjalności, podwójne powiadomienie o pozostawieniu przesyłki awizo) w stosunku do stron nie-

będących podmiotami publicznymi mają na celu chronić je przed skutkami zaniechań. W przypadku podmiotów publicznych ich sposób działania i pracy regulują normy prawa ustrojowego oraz normy zadaniowe zawarte w ustawach. Takimi normami są przepisy ustawy o informatyzacji. Kodeks postępowania administracyjnego nie reguluje wszystkich aspektów informatyzacji tych podmiotów, wprost odwołując do ustawy o informatyzacji, co potwierdza tezę, że wolą ustawodawcy w zakresie doręczeń elektronicznych należy stosować zasady przewidziane w ustawie o informatyzacji oraz aktach wykonawczych wydanych na jej podstawie.

Słowa kluczowe: doręczenie decyzji, Kodeks postępowania administracyjnego, elektroniczna skrzynka podawcza, doręczenie pomiędzy podmiotami publicznymi.

E-delivery between public entities during a proceeding

In the present commentary the author discusses two rulings of the Supreme Administrative Court regarding e-deliveries between public entities during a proceeding, to which the provisions of the Code of Administrative Procedure apply. The Supreme Administrative Court recognized that the day of a delivery of an administrative act to a public authority is the day of acknowledgment by putting an e-signature by a clerk, and not the day of the confirmation of submission issued by the electronic mailbox. The commentary describes two rulings based on a similar factual state and similar motions. An important argument was also the fact that the voted rulings are relatively new. The commentary is also critical towards conclusions presented by the Supreme Administrative Court. In the author's opinion the rulings do not take into account the specifics of public entities – even if they appear as a party to administrative proceedings and provisions of the act of 17.2.2005 on computerization of activities of entities pursuing public tasks.

Keywords: delivering ruling, administrative code, electronic mailbox, delivery between public entities.



Bezpieczeństwo danych



www.ksiegarnia.beck.pl

Zadzwonić: 81 46 13 300 • E-mail: kontakt@beck.pl

WYMOGI EDYTORSKIE:

- język publikacji: polski, angielski, niemiecki, rosyjski;
- edytor tekstu Word (format .doc lub .docx);
- styl czcionki: Times New Roman;
- wielkość czcionki: tekst główny – 12 pkt, przypis – 10 pkt;
- interlinia: 1,5 wiersza (w przypadku przypisów – 1 wiersz);
- objętość artykułu: do 30 000 tys. znaków ze spacjami;
- marginesy: standardowe – wszystkie 2,5 cm;
- przypisy dolne: odsyłaczami przypisów powinny być cyfry arabskie; odsyłacz należy umieścić bezpośrednio po fragmencie, do którego odnosi się przypis (przed kropką kończącą zdanie);
- należy dołączyć słowa kluczowe w języku polskim i angielskim;
- tytuł powinien być napisany czcionką Times New Roman 14 pkt (czcionka pogrubiona);
- tekst powinien składać się z następujących części: lid (streszczenie ok. 1500 znaków ze spacjami), uwagi wstępne, rozwinięcie (z podziałem na zatytułowane części), podsumowanie;
- do artykułu należy załączyć także lid (streszczenie) w języku angielskim (ok. 1500 znaków ze spacjami);
- śródtytuły nie powinny być numerowane, lecz pogrubione;
- należy dołączyć notę biograficzną (ok. 800 znaków ze spacjami);
- prosimy o wskazanie afiliacji.

Powoływane w przypisach pozycje bibliograficzne prosimy pisać według wzoru:

Inicjał. Nazwisko, Tytuł, ew. numer wydania, tom, część itp., miejsce i rok wydania, a następnie cytowane strony skrótem „s.”, np.: *J. Kowalski*, Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku kolejnego powołania się **bezpośrednio** na cytowaną pozycję:

Ibidem, s. 15–16.

Powołanie kolejny raz, gdy cytujemy tylko jedną pozycję danego autora:

J. Kowalski, *op. cit.*, s. 29–20.

Kolejne powołanie, gdy cytuje się kilka pozycji danego autora, zawiera pierwsze wyrazy tytułu, np.:

J. Kowalski, Jak pisać..., s. 28–29.

W przypadku **prac pod redakcją**, jeśli powoływana publikacja stanowi część całości:

P. Igrak, Cytowanie, [w:] *J. Kowalski* (red.), Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku publikacji w czasopiśmie tytuł czasopisma zastępuje nazwę wydawnictwa, po nim następuje rok (rocznik), przecinek, następnie numer (nr) w ramach rocznika ewentualnie także numer od początku wydawania pisma i numer strony:

J. Kowalski, Jak pisać przypisy?, *Wiadomości Tekściarskie* 2006, Nr 28 (236), s. 7.

Kilka kwestii specjalistycznych:

1. Oczekiwane oznaczenie ustawy wygląda następująco: Dz.U. z 2006 r. Nr 28, poz. 456.
2. Publikator prosimy podawać jedynie przy pierwszym przywołaniu aktu prawnego. Wówczas nazwę aktu i datę (miesiąc słownie) podajemy w tekście głównym (np. ustawa z 13.4.2003 r. o zasadach pisanie artykułów), w przypisie zaś publikator (np. t.j. Dz.U. z 2006 r. Nr 28, poz. 456).
3. Zapisując artykuł, ustęp, punkt aktu prawnego, skrótów nie odzielamy przecinkami, tak więc: art. 28 ust. 59 pkt (bez kropki!) 36, a nie: art. 28, ust. 59, pkt. 36.
4. W przypadku orzeczeń sądowych prosimy o zastosowanie następujących oznaczeń: Wyrok SN z 11.5.2011 r., I CA 123/11, OSNCP 2011, Nr 8, poz. 34. Nazwę orzeczenia i jego datę prosimy podać w tekście głównym (np. wyrok SN z 11.5.2011 r.), natomiast w przypisie publikator (I CA 123/11, OSNCP 2011, Nr 8, poz. 34).

Harmonogram publikacji:

Nr 1 – teksty do końca stycznia, druk luty/marzec

Nr 2 – teksty do końca kwietnia, druk maj/czerwiec

Nr 3 – teksty do końca lipca, druk sierpień/wrzesień

Nr 4 – teksty do końca października, druk listopad/grudzień

Osoba do kontaktu: dr *Aleksandra Klich*, e-mail: pme@beck.pl

EDITORIAL REQUIREMENTS:

- language of publication: Polish, English, German, Russian;
- text editor MS Word (.doc or .docx);
- font style: Times New Roman;
- font size: main text – 12 pts, footnote – 10 pts;
- line spacing: 1.5 line (for footnotes – 1 row);
- volume of the article: up to 30,000 characters with spaces;
- margins: standard – all 2.5 cm;
- footnotes: cross-referenced footnotes should be Arabic numerals; reference should be placed immediately after the passage to which the footnote regards (before the full stop ending a sentence);
- article must be attached with key words in Polish and English;
- the title should be written in Times New Roman 14 pts (bold);
- text should consist of following parts: lead (summary, around 1500 characters with spaces), initial comments, amplification (with a division into parts with titles), summation;
- article should also be attached with a lead (summary) in English (around 1500 characters with spaces);
- intertitles should not be numbered, but bold;
- article must be attached with a biographical note (approx. 800 characters including spaces);
- please indicate affiliation.

The referenced sources should adhere to the following style:

Initial(s). Last name, Title, edition number if applicable, volume, part, etc., place and year of publication, followed by the page(s) referred to with the 'p. (pp.)' abbreviation, e.g.: *J. Kowalski*, How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For subsequent reference made **directly** to the cited item:

Ibidem, p. 15–16.

Further reference, when several positions by a given author are being cited, include the first words of the title, e.g.:

J. Kowalski, How to..., p. 28–29.

For edited volumes, when the publication referenced forms a part of the whole:

P. Igrak, Citing, [in:] *J. Kowalski* (ed.), How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For publications in periodicals, the title of the periodical replaces the name of the publisher, followed by the year, comma, then the number (No.) within the year, possibly the consecutive number and page numbers:

J. Kowalski, How to do references?, *Editorial news* 2006, No. 28 (236) p. 7.

A few technical issues:

- a. Expected indication of a legal act goes as follows:
Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April on the rules of writing articles), and the publishing body shall be given in the footnote (e.g. Journal of Laws of 2006, No. 28, item 456).
- b. When writing article, paragraph, point of a legal act, abbreviations should not be separated by commas, that is: art. 28 par. 59 point (no full stop!) 36, not: art. 28, par. 59, pt. 36).
- c. For court judgements, please use the following indications: Judgement of the Supreme Court of 11.5.2011, I CA 123/11, OSNCP 2011, No. 8, item 34. Mind that the appellation of the judgement and its date should be indicated in the main text (e.g. Judgement of the Supreme Court of 11.5.2011), and the publishing body in the footnote (I CA 123/11, OSNCP 2011, No. 8, item 34).

Publication schedule (deadlines):

No. 1 – submitting manuscripts – end of January (print – February/March)

No. 2 – submitting manuscripts – end of April (print – May/June)

No. 3 – submitting manuscripts – end of July (print – August/September)

No. 4 – submitting manuscripts – end of October (print – November/December)

Contact Person: *Aleksandra Klich* PhD, e-mail: pme@beck.pl