e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

Podręcznik e-Commerce Polska

Rewolucja w ochronie danych osobowych?

Istotne zmiany dla przedsiębiorcy

Izba Gospodarki Elektronicznej
Warszawa, 2016

Redaktor wydania: Łukasz Kiczma

Współpraca merytoryczna:

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Słowem wstępu…

Izba Gospodarki Elektronicznej (dalej: e-Izba) z przyjemnością oddaje w Państwa ręce kolejny Podręcznik e-Commerce Polska: *Rewolucja w ochronie danych osobowych? Istotne zmiany w ochronie danych osobowych dla przedsiębiorcy*. W tym podręczniku pragniemy zwrócić uwagę na wybrane rozwiązania szczegółowe o istotnym znaczeniu dla przedsiębiorców, jakie znalazły się w zapisach RODO. Do najważniejszych należą takie problemy jak:

- Obowiązki notyfikacyjne administratora
- Przetwarzanie danych wrażliwych
- Brak obowiązku zgłaszania zbiorów danych osobowych
- „Rozliczalność" *przestrzegania zasad przetwarzania danych osobowych*
- Nowe obowiązki informacyjne
- Administratorzy bezpieczeństwa informacji
- Ograniczenie automatycznego profilowania
- Prawo przenoszenia danych
- Prawo do bycia zapomnianym
- Cywilnoprawna odpowiedzialność administratora danych
- Kwestia kluczowa: surowe kary administracyjne

Wybrane zagadnienia z powyższej listy tematów prawnych związanych z wdrożeniem w życie RODO, w swoich artykułach omawiają prawnicy kancelarii partnerskich e-Izby: DLA Piper Wiater sp.k., Kancelaria Chabasiewicz Kowalska i Partnerzy, **Kancelaria Radcy Prawnego Marek Wiński**, Lubasz i Wspólnicy Kancelaria Radców Prawnych sp.k., Szostek_Bar i Partnerzy Kancelaria Prawna.

> *„Analiza przepisów RODO pozwala twierdzić, że jest to istotna zmiana, choć nie ma ona charakteru rewolucji. Od strony przedsiębiorców o potrzebie szczególnej rewizji dotychczasowych praktyk stanowią naturalnie grożące, w przypadku naruszenia zasad przetwarzania danych, sankcje. Istnieje również obawa, że stosowanie przepisów RODO wiązać będzie się z dodatkowymi kosztami, m.in. implementacji systemów certyfikacyjnych, etc. Z kolei z perspektywy organów władzy publicznej RODO oznacza w szczególności*

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

konieczność dostosowania krajowego ustawodawstwa" – mówi radca prawny Agata Kowalska z Kancelarii Chabasiewicz Kowalska i Partnerzy.

Zapraszamy również Państwa do wspólnego tworzenia i rozwijania polskiej branży e-commerce. e-Izba reprezentuje i wspiera interesy firm związanych z rynkiem gospodarki elektronicznej w Polsce, ze szczególnym uwzględnieniem firm zrzeszonych.

Misją e-Izby jest rozwój polskiej branży e-commerce poprzez współpracę, wymianę know-how, działania legislacyjne oraz silną i efektywną reprezentację wspólnych interesów w dialogu z instytucjami polskiej administracji rządowej, Unii Europejskiej oraz organizacjami pozarządowymi w kraju i na świecie. Główne cele e-Izby to:

- reprezentowanie i wspieranie interesów gospodarczych firm związanych z rynkiem gospodarki elektronicznej w Polsce, ze szczególnym uwzględnieniem firm zrzeszonych w e-Izbie,
- rozwój gospodarki w różnych jej branżach w kraju i Europie dzięki wykorzystaniu innowacji technologicznych, informacyjnych i komunikacyjnych (ICT), w tym sieci Internet oraz sprzętu i oprogramowania oraz ich praktycznych zastosowań w prowadzeniu działalności gospodarczej, wspieranie przedsiębiorców (zwłaszcza małych i średnich) poprzez dostarczanie wiedzy (know-how) oraz rozwiązań technologicznych,
- wspieranie społeczeństwa w korzystaniu z rozwiązań cyfrowych.

Wierzymy, że mając podobne potrzeby w zakresie aktywności, takich jak regulacje prawne, badania trendów, wypracowywanie standardów rynkowych czy działania edukacyjne w kontekście rzeczywistych wyzwań branży, możemy wspólnymi siłami rozwijać branżę gospodarki elektronicznej.

Z poważaniem,

/-/ Łukasz Kiczma

Pełnomocnik Zarządu
Izby Gospodarki Elektronicznej
ds. legislacji krajowej

Warszawa, 2016-06-13

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Spis treści

Słowem wstępu… 3

Chomiczewski W., Przetwarzanie danych biometrycznych w RODO 6

Klimas D., Sankcje o charakterze pieniężnym za naruszenie zasad ochrony danych osobowych według UODO i RODO 9

Koellner T., Odpowiedzialność administracyjnoprawna z tytułu naruszenia zasad przetwarzania danych osobowych na gruncie Ogólnego Rozporządzenia o Ochronie Danych Osobowych 16

Lubasz D. dr, Przesłanki legalizacyjne przetwarzania danych osobowych 19

Pękała M., Koniec dowolności przy profilowaniu danych osobowych 23

Tobiczyk P., Zasada rozliczalności - nowe wyzwanie dla branży 27

Wiński M., Co dotyczy Unii zostaje w Unii, czyli jednolity zakres stosowania Ogólnego Rozporządzenia o ochronie danych osobowych w Unii Europejskiej 30

Witkowska K., Inspektor ochrony danych na gruncie RODO 34

Zawadzka N., Prawo do bycia zapomnianym na gruncie ogólnego rozporządzenia o ochronie danych osobowych 38

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Chomiczewski Witold, radca prawny
LUBASZ I WSPÓLNICY KANCELARIA RADCÓW PRAWNYCH SP.K.

Przetwarzanie danych biometrycznych w RODO

W dzisiejszym obrocie coraz częściej spotyka się rozwiązania oparte na danych biometrycznych. Pojawiają się zwłaszcza jako forma zabezpieczenia przed dostępem osób nieuprawnionych do szczególnie ważnych informacji w ramach przedsiębiorstw. Rozwijane są również technologie autoryzacji płatności z wykorzystaniem danych biometrycznych, jako odpowiedź na uproszczenie akceptacji płatności przy zachowaniu najwyższego poziomu bezpieczeństwa. Praktyka pokazuje jednak, że rozwiązania oparte o dane biometryczne pojawiają się również przykładowo przy rejestracji czasu pracy.

W ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1] zagadnienie danych biometrycznych nie jest bezpośrednio regulowane. Dane te są po prostu kwalifikowane jako dane osobowe w rozumieniu art. 6 ustawy, natomiast nie mają własnej definicji. Ograniczenie wykorzystania danych biometrycznych było do tej pory wyprowadzane z wyrażonej w art. 26 ust. 1 pkt 3 ustawy zasady adekwatności i proporcjonalności zbieranych danych osobowych do celu, w którym są przetwarzane. Na tej podstawie uznawano m.in., że systemy rejestracji czasu pracy w oparciu o odczyt linii papilarnych, czy siatkówki oka, są nieproporcjonalne oraz nieadekwatne dla realizacji takiego celu. Było tak ze względu na możliwość zastosowania rozwiązań mniej ingerujących w prywatność pracowników, jak przykładowo rejestracja w oparciu o indywidualne karty magnetyczne lub tradycyjne podpisy na liście.

Rozporządzenie ogólne[2], w odróżnieniu od ustawy o ochronie danych osobowych, zawiera regulacje dotyczące danych biometrycznych. W art. 4 pkt 14 Rozporządzenia ogólnego dane biometryczne zostały zdefiniowane jako dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Prawodawca unijny nie zdecydował się zatem na ujęcie danych biometrycznych w zamkniętym katalogu poprzez precyzyjne wymienienie ich kategorii. Zastosowane zostało elastyczne

[1] Dz.U. 2015 r. poz. 2135.
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1).

rozwiązanie polegające na wskazaniu trzech cech danych biometrycznych: technicznego przetwarzania, odnoszącego się do cech fizycznych, fizjologicznych lub behawioralnych człowieka, które pozwalają na jednoznaczną jego identyfikację. Wszystkie dane osobowe spełniające te cechy będą kwalifikowane jako dane osobowe biometryczne. Jedynie przykładowo wymienione zostały dwie kategorie takich danych: wizerunek twarzy oraz dane daktyloskopijne.

Tak rozumiane dane biometryczne zostały zakwalifikowane przez prawodawcę unijnego jako dane osobowe szczególnej kategorii w rozumieniu art. 9 Rozporządzenia ogólnego. Oznacza to, że dane biometryczne są chronione tak samo, jak dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne lub światopoglądowe, przynależność do związków zawodowych i dane genetyczne. Na postawie art. 9 ust. 1 Rozporządzenia ogólnego obowiązuje zakaz przetwarzania danych osobowych biometrycznych. Przepis art. 9 ust. 2 wymienia wyjątki od powyższego zakazu i dopuszcza przetwarzanie danych biometrycznych w m.in. w następujących sytuacjach[3]:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
3. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
4. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Wobec powyższego przetwarzanie danych biometrycznych będzie możliwe jedynie wówczas, gdy spełniona będzie przynajmniej jedna z przesłanek wymienionych w art. 9 ust. 2 Rozporządzenia ogólnego.

Ochrona danych biometrycznych została potraktowana w Rozporządzeniu ogólnym bardzo poważnie, gdyż niezależnie od ich kwalifikacji jako danych osobowych szczególnej kategorii, a zatem poddanych dalej idącej ochronie, prawodawca unijny dopuścił dodatkowe zaostrzenie ich zabezpieczenia przez państwa członkowskie. Uprawnienie do zaostrzenia ochrony daje państwom członkowskim przepis art. 9 ust. 4 Rozporządzenia ogólnego. W konsekwencji Polska będzie mogła wprowadzić jeszcze

[3] ze względu na ramy niniejszego opracowania wskazywane są najważniejsze przesłanki legalizujące przetwarzanie danych biometrycznych.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

większe ograniczenia w przetwarzaniu danych osobowych biometrycznych, niż wynikające z Rozporządzenia ogólnego.

Witold Chomiczewski LL.M, radca prawny - lider specjalizacji E-Commerce w Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp. k.

Specjalizuje się w prawie IT i nowych technologii. Posiada bogate doświadczenie w obsłudze prawnej przedsiębiorców związanych z E-Commerce. Doradza m.in. spółkom zajmującym się marketingiem internetowym. Przygotowuje umowy z zakresu SEO/SEM, reklamy RTB, prawa autorskiego w Internecie.

Wspiera przedsiębiorców internetowych, a zwłaszcza portale, w sprawach związanych z odpowiedzialnością za cudze treści.

Posiada doświadczenie w prowadzeniu postępowań sądowych z zakresu prawa autorskiego, Internetu oraz prawa gospodarczego.

Brał udział w projekcie na zlecenie KE, *Study on Liability of Internet Intermediaries*, który dotyczył dyrektywy o handlu elektronicznym.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Klimas Damian
SZOSTEK_BAR I PARTNERZY KANCELARIA PRAWNA

Sankcje o charakterze pieniężnym za naruszenie zasad ochrony danych osobowych według UODO i RODO

"BEZKARNOŚĆ" ADO

Na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 z późn. zm.) (dalej: UODO) wielu administratorów danych osobowych (dalej: ADO), czyli przedsiębiorców prowadzących sklepy internetowe, osób prowadzących kampanie marketingowe swojej działalności gospodarczej, podmiotów świadczących usługi płatnicze itp., czuje się bezkarnie. Naruszenie prawa ochrony danych osobowych może przybrać różną postać. Jest to między innymi niezgłoszenie zbioru danych osobowych do rejestru prowadzonego przez Głównego Inspektora Danych Osobowych (dalej: GIODO), niewłaściwe zabezpieczenie danych osobowych, nieupoważnione udostępnienie danych osobowych osobom trzecim, przetwarzanie danych osobowych w zbiorze mimo niedopuszczalności takiej działalności. ADO pomimo pełnej świadomości naruszania prawa, decydowali się na jego łamanie z uwagi na niski wymiar kar pieniężnych nakładanych przez GIODO.

UPRAWNIENIA GIODO NA GRUNCIE UODO

UODO za przetwarzanie danych osobowych w sposób niezgodny z prawem przewiduje odpowiedzialność administracyjną, a także karną osoby, która przetwarza dane niezgodnie z prawem. Niemniej jednak w razie stwierdzenia naruszenia przepisów ustawy GIODO nie został uprawniony do nakładania sankcji na osoby odpowiedzialne za niezgodne z UODO przetwarzanie danych osobowych. Art. 18 UODO wskazuje na uprawnienia GIODO, które ograniczają się do merytorycznego rozstrzygania sprawy w formie decyzji administracyjnej nakazującej przywrócenie stanu zgodnego z prawem. Oznacza to, że GIODO ma prawo nakazać przedsiębiorcy prowadzącemu sklep internetowy, aby ten (przywracając stan zgodności z prawem) zarejestrował bazę danych albo żeby poprawił formułę oświadczenia składanego przez osobę, której dane osobowe będą przetwarzane (składane pod formularzem w którym zostawia się podstawowe dane, w formie zaznaczenia popularnego *checkboxa*).

GIODO może zatem (zarówno na wniosek osoby zainteresowanej, jak i z urzędu) nałożyć obowiązek uzupełnienia, uaktualnienia, sprostowania, udostępnienia lub nieudostępnienia danych osobowych (szczególnie na wniosek osoby, której dane są przetwarzane); zastosowania dodatkowych środków zabezpieczających zgromadzone dane osobowe lub ich zabezpieczenie (zainstalowanie

odpowiedniego oprogramowania antywirusowego na serwerze na którym dane są przetwarzane, "zainstalowanie" certyfikatu SSL, zastosowanie szyfrowania, lub zmianę haseł na trudniejsze do "złamania"), a także usunięcie danych osobowych (szczególnie jeśli osoba weszła w ich posiadanie w sposób niezgodny z prawem, na przykład nie uzyskując odpowiedniej zgody osób, których dane są przetwarzane).

Mylnie uważa się, że GIODO ma legitymację do karania. Z uwagi na to, że UODO wprost określa uprawnienia GIODO (art. 12 i 18 UODO), w razie stwierdzenia naruszenia prawa ochrony danych osobowych, należy podkreślić, że GIODO nie ma uprawnień do karania osób odpowiedzialnych za to naruszenie. Jednakże na podstawie z art. 12 ust. 3 UODO, GIODO ma uprawnienia organu egzekucyjnego w zakresie egzekucji obowiązków o charakterze niepieniężnym. Czyli jeśli przedsiębiorca naruszy postanowienia UODO, będzie musiał przywrócić stan zgodności z prawem (np. zarejestrować zbiór danych osobowych), a GIODO może nałożyć na niego grzywnę przymuszającą, aby tego przedsiębiorcę "zmotywować".

WYSOKOŚĆ GRZYWNY PRZYMUSZAJĄCEJ

Warto podkreślić, że UODO nie reguluje wysokości grzywien, ani kar finansowych, a jedynie "wysokość" sankcji karnych. To jak wysoką grzywnę GIODO może nałożyć reguluje ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tj. z 2014 r. poz. 1619 z późn. zm.) (dalej PostEgzAdmU). Zgodnie z jej postanowieniami kary administracyjne (finansowe) za nieprzestrzeganie zasad dotyczących ochrony danych osobowych mogłyby przez niektórych być uznawane za dotkliwe. GIODO ma bowiem prawo nałożyć grzywnę przymuszającą w wysokości do 10 tys. zł dla osób fizycznych, a także do 50 tys. zł dla osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej. Od 2011 roku, w przypadku wielokrotnego nakładania grzywien w jednym postępowaniu egzekucyjnym ich łączna kwota nie może przekraczać odpowiednio 50 tys. zł dla osób fizycznych oraz 200 tys. zł dla osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej. Trzeba wskazać, że jedynie niepodporządkowywanie się przez długi okres czasu kolejnym wezwaniom GIODO może skutkować tak wysokiej karze nałożonej na przedsiębiorcę (200 tys. zł). Za jednorazowe przewinienie, które tym samym jest bardzo poważne, GIODO może nałożyć grzywnę jedynie w wysokości 50 tysięcy złotych. Rzadko zdarzały się jednak tak poważne naruszenia przepisów, częściej GIODO nakładał bowiem niższe grzywny.

W przypadku gdy zobowiązany podmiot nie podporządkuje się decyzji GIODO w zakresie przywrócenia stanu zgodnego z prawem, do zadań GIODO należy zapewnienie wykonania obowiązku

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

przez zastosowanie środków egzekucyjnych przewidzianych w PostEgzAdmU. Podstawowym naruszenie zadaniem GIODO jest bowiem zapewnienie przywrócenia stanu zgodnego z prawem. Grzywna jest jedynie środkiem, który ma zapewnić przywrócenie tego stanu.

ODPOWIEDZIALNOŚĆ KARNA WEDŁUG UODO

Odpowiedzialność karna za naruszenie ochrony danych osobowych została uregulowana w art. 49–54a UODO. Odpowiedzialność tą ponoszą zawsze osoby fizyczne, którym można przypisać odpowiedzialność, z uwagi na specyfikę prawa karnego. Przestępstwa "nie może" popełnić osoba prawna, bowiem ta odpowiedzialność zawsze będzie przypisana osobie (lub osobom) fizycznej. Jeśli przestępstwo jest związane z tzw. podmiotem zbiorowym (a więc osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej), w grę będą wchodziły przepisy ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz.U. z 2015 r. poz. 1212 z późn. zm.). Ustawa ta wskazuje jakie osoby fizyczne są odpowiedzialne za działanie "podmiotu zbiorowego".

Dość powszechnie wskazuje się, że "system przepisów karnych [UODO] (...) jest mało efektywny jako narzędzie służące do zapewnienia przestrzegania przepisów UODO" (tak komentarz do rozdziału 8 UODO, Barta w: Ustawa o ochronie danych Osobowych. Komentarz, red. Barta, Litwiński, Warszawa 2016). Autor wskazuje, że regulacja odpowiedzialności karnej jest nieskuteczna, z uwagi na określenie przestępstw w znacznej części jako typów czynów zabronionych, które muszą być popełnione umyślnie, a także powszechne uznanie naruszenia UODO (np. niezgłoszenie zbioru danych osobowych do rejestracji, czy naruszenie obowiązków informacyjnych względem osób, których dane dotyczą) za działanie (a głównie zaniechanie), które nie powinno być uznane za przestępcze. Wielokrotnie postulowano, aby odejść od odpowiedzialności karnej, na rzecz nakładania odpowiednio wysokich sankcji pieniężnych.

REFORMA ODPOWIEDZIAL**NOŚCI W RODO**

Prawodawca unijny uznał, że aby egzekwowanie przepisów GDPR było skuteczniejsze, należy za jego nakładać odpowiednie sankcje, w tym kary pieniężne o charakterze administracyjnym. Sankcje te mają być nakładane zamiast lub obok odpowiednich środków nakładanych na mocy RODO przez organ nadzorczy.

Od rozpoczęcia obowiązywania RODO GIODO będzie miał nie tylko prawo do merytorycznego rozstrzygnięcia sprawy, ale także prawo do samodzielnego nałożenia kary pieniężnej na podmiot

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

naruszający prawo ochrony danych osobowych. Znacząco zmieni to pozycję tego organu, bowiem uprawnienie do nakładania kar pieniężnych (szczególnie tak dotkliwych), jest ogromnym wzmocnieniem funkcji nadzorczej, jaką pełni GIODO.

Oczywiście nakładanie sankcji, w tym administracyjnych kar pieniężnych, będzie podlegało odpowiednim zabezpieczeniom proceduralnym zgodnym z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych, w tym skutecznej ochronie prawnej i prawu do rzetelnego procesu. Wszystko to ma na celu, aby GIODO nie miał swobodnego uznania w zakresie tego na kogo nałoży karę, a także swobody w zakresie wyboru wysokości tej kary. Mogłoby to bowiem doprowadzić do daleko idących nieprawidłowości, które mogłyby z kolei pociągnąć za sobą skutek w postaci np. wykluczenia jakiegoś rodzaju podmiotów.

W RODO zastosowano dwa limity kar pieniężnych w zależności od rodzaju naruszenia prawa ochrony danych osobowych. Pierwszy limit, to kara wynosząca do 10 000 000 Euro, a w przypadku przedsiębiorstwa do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Drugi limit, to kara wynosząca do 20 000 000 Euro, a w przypadku przedsiębiorstwa do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku.

Dwa limity wysokości kar pieniężnych

Niższy limit kar przewidziany jest za naruszenie całego szeregu obowiązków administratorów danych lub podmiotów przetwarzających, w tym m.in. naruszenia:

1) obowiązku uzyskania odpowiedniej zgody od opiekuna osoby fizycznej poniżej 16 roku życia w przypadku oferowania jej usług społeczeństwa informacyjnego (np. dostępu do portalu społecznościowego)

2) uwzględniania ochrony danych osobowych w fazie projektowania (*privacy by design*)

3) wdrożenia odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne dla osiągnięcia celu przetwarzania (*privacy by default*);

4) obowiązku zgodnej z RODO wewnętrznej regulacji przetwarzania danych przez dwóch lub więcej ADO;

5) a także m.in. obowiązków:

a) przetwarzania danych z upoważnienia ADO,
b) współpracy GIODO,
c) rejestrowania przetwarzania danych,
d) zabezpieczenia danych w odpowiedni sposób,

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

e) zawiadamiania GIODO o naruszeniach prawa ochrony danych osobowych,

f) uprzedniej konsultacji z GIODO w określonych sytuacjach.

6) zasad dobrowolnej certyfikacji wskazującej na wysoką jakość w zakresie ochrony danych osobowych świadczącej o zgodności z RODO operacji przetwarzania prowadzonych przez ADO.

Wyższy limit kar dotyczy naruszenia poważnych obowiązków, a w szczególności naruszenia:

a) podstawowych zasad przetwarzania, w tym warunków zgody, przetwarzania zgodnego z prawem, rzetelnego i przejrzystego, a także adekwatności, prawidłowości i konkretności przetwarzania danych (szerzej - art. 5, 6, 7 oraz 9 RODO);

b) praw osób, których dane dotyczą, a w szczególności przejrzystego informowania o przetwarzaniu, komunikacji, zakresu informacji o ADO, prawo dostępu do danych, sprostowania, usunięcia i ograniczenia przetwarzania, a także powiadomienia o tych faktach, prawo do przenoszenia danych, a także sprzeciwu oraz nie podlegania decyzji opierającej się o zautomatyzowane przetwarzanie (szerzej - art. 12–22 RODO);

c) przekazywania (transferu) danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej (szerzej art. 44–49 RODO);

d) wszelkich obowiązków, które mogą wynikać z prawa Polskiego, które dostosuje RODO do polskiego porządku prawnego;

e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 RODO lub niezapewnienia dostępu do danych skutkującego naruszeniem art. 58 ust. 1 RODO.

Wskazane naruszenia ochrony danych osobowych są na gruncie UODO powszechne wśród przedsiębiorców działających w branży eCommerce. Na wstępie wyjaśniono pokrótce dlaczego tak się dzieje, ale wszystko wskazuje na to, że taki stan rzeczy nie będzie się długo utrzymywał. Prawodawca unijny wytoczył działa najwyższego kalibru do walki z naruszeniami ochrony danych osobowych, więc przedsiębiorcy wykorzystujący środki komunikacji elektronicznej do marketingu i świadczenia usług będą ze strachu przed dotkliwą sankcją wypełniali należycie obowiązki wynikające z RODO.

Warto na marginesie zauważyć, że polski ustawodawca będzie mógł określić, czy w ogóle, a jeśli tak, to w jakim zakresie kary pieniężne GIODO będzie mógł nakładać na organy administracji publicznej w Polsce. Można się zatem spodziewać, że polskie organy administracji publicznej będą ponosiły co najwyżej ograniczoną odpowiedzialność z tytułu naruszenia RODO.

WYMIAR KARY PIENIĘŻNEJ WEDŁUG RODO

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

W RODO prawodawca daje wskazówki dla GIODO i ADO w zakresie wymiaru kary pieniężnej. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, będzie można zamiast tego udzielić upomnienia. GIODO będzie miał obowiązek zapewnienia, aby kary pieniężne były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

Zgodnie z RODO GIODO będzie musiał zwrócić należytą uwagę:

a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
b) na to, czy naruszenie było umyślne, czy nie;
c) na działania podjęte dla zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
d) na stopień odpowiedzialności;
e) na stopień współpracy z GIODO w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
f) stosowanie zatwierdzonych kodeksów postępowania;
g) wszelkie mające znaczenie wcześniejsze naruszenia;
h) na sposób, w jaki organ nadzorczy dowiedział się o naruszeniu;
i) kategorie danych osobowych, których dotyczyło naruszenie;
j) na przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający;
k) na stosowanie kodeksów postępowania oraz wszelkie inne czynniki obciążające lub łagodzące, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

PODSUMOWANIE

Zdaniem podsumowania należy uznać, że RODO w zakresie kształtowania zasad odpowiedzialności i kar administracyjnych, które będzie mógł nałożyć GIODO znacząco wpływa na ryzyko prowadzenia działalności gospodarczej. Sankcje proponowane przez RODO są kilkadziesiąt lub nawet kilkaset razy większe niż do tej pory proponowane przez ustawodawcę polskiego.

Warto również zauważyć, iż mimo regulacji kwestii odpowiedzialności za szkodę zawartej w ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U z 2016 r. poz. 380 z późn. zm.) (dalej jako KC), RODO w art. 82 znacząco rozszerza tą tradycyjnie przez KC ujętą odpowiedzialność. Zgodnie z

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

powołanym artykułem, każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO będzie miała prawo uzyskać od ADO lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. ADO lub podmiot przetwarzający będą mogli zwolnić się z odpowiedzialności dopiero jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Zatem nawet przyczynienie się do szkody będzie skutkowało odpowiedzialnością z tego tytułu.

Podmioty działające w branży eCommerce muszą się zatem mieć na baczności i już teraz rozpocząć przygotowania do wprowadzenia odpowiednich polityk bezpieczeństwa oraz instrukcji, a także dogłębnego przeszkolenia swoich pracowników i współpracowników. Naruszanie prawa przestanie być bowiem bezkarne, a obowiązkiem GIODO nałożonym przez prawodawcę unijnego będzie doprowadzenie do stanu, w którym polscy przedsiębiorcy będą dochowywali obowiązków określonych w prawie ochrony danych osobowych. Narzędziem dla tego celu mają być między innymi opisane wyżej sankcje.

Klimas Damian, Associate w kancelarii prawnej Szostek_Bar i Partnerzy, doktorant w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

W ramach pracy zawodowej zajmował się w szczególności świadczeniem bieżącej pomocy prawnej w dziale compliance międzynarodowej grupy kapitałowej z zakresu prawa handlowego, prawa papierów wartościowych, prawa ochrony danych osobowych oraz prawa autorskiego. Był również członkiem zespołu prawnego przygotowującego emisję obligacji korporacyjnych.

Posiada znaczące doświadczenie w kompleksowej obsłudze spółek, sporządzaniu umów, a także opinii prawnych. Prelegent na konferencjach ogólnopolskich i międzynarodowych, szkoleniowiec, autor publikacji naukowych z zakresu prawa mediów elektronicznych, w tym ochrony danych osobowych, prawa konsumenckiego w obrocie elektronicznym, prawa e-reklamy oraz prawa autorskiego.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Koellner Tomasz, aplikant adwokacki
KANCELARIA CHABASIEWICZ KOWALSKA I PARTNERZY

Odpowiedzialność administracyjnoprawna z tytułu naruszenia zasad przetwarzania danych osobowych na gruncie Ogólnego Rozporządzenia o Ochronie Danych Osobowych

Ogólne rozporządzenie o ochronie danych osobowych – **określane skrótowo jako RODO – stanowi rewolucję w zakresie obowiązującego systemu ochrony danych osobowych, prowadząc w szczególności do jego ujednolicenia w skali Unii Europejskiej. Nie ulega wątpliwości, że RODO** spowoduje ba**rdzo istotny wzrost znaczenia reguł przetwarzania danych osobowych w codziennej praktyce przedsiębiorców. Co więcej, tendencja ta jest już obecnie wyraźnie zauważalna** – firmy **podejmują działania mające przygotować je na wejście w życie nowych przepisów, co nastąpi wiosną 2018 r. Stanowi to przede wszystkim wynik diametralnej zmiany podejścia regulacyjnego do sankcji administracyjnych z tytułu naruszenia zasad przetwarzania danych, skutkującej znaczącym zaostrzeniem odpowiedzialności administratorów i innych podmiotów dokonujących** operacji na danych osobowych.

Dotychczasowy kształt regulacji obowiązujących w Polsce, a także w innych krajach Unii Europejskiej, powoduje, że prowadzona u przedsiębiorcy kontrola w zakresie zgodności przetwarzania danych z prawem budzi znacznie mniejsze obawy, aniżeli analogiczne postępowania kontrolne prowadzone przez inne organy nadzoru – w tym przykładowo przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów.

Podczas gdy drugi z wymienionych organów, obok możliwości wydania w pewnych przypadkach decyzji nakazowej, dysponuje również uprawnieniem do nakładania surowych kar administracyjnych, sięgających nawet 10% obrotu osiągniętego przez przedsiębiorcę w roku poprzedzającym rok nałożenia kary, Generalny Inspektor Ochrony Danych Osobowych (GIODO) dotychczas był tej możliwości pozbawiony, a jego instrumentarium ograniczało się zasadniczo do wydania decyzji nakazującej usunięcie naruszeń stwierdzonych w toku kontroli.

Dopiero brak wykonania powyższej decyzji (która częstokroć wykonywana była jeszcze w toku postepowania wyjaśniającego, skutkując jego umorzeniem), umożliwiał GIODO sięgnięcie do środków represyjnych, przewidzianych w ustawie o postępowaniu egzekucyjnym w administracji – tj. do tzw. grzywny w celu przymuszenia. Grzywna ta wynieść mogła maksymalnie 10.000 zł w stosunku do osoby

fizycznej lub 50.000 zł w stosunku do osoby prawnej, a łączna wysokość kar (nakładanych wielokrotnie) nie mogła przekroczyć odpowiednio 50.000 zł i 200.000 zł. Oczywiście obok sankcji administracyjnych dotychczasowe regulacje przewidują również sankcje karne, jednak te stosowane były jedynie w szczególnie rażących przypadkach naruszenia przepisów ustawy o ochronie danych osobowych.

Opisane wyżej podejście, które niewątpliwie określić można mianem łagodnego i nastawionego na wymuszenie dostosowania praktyk do obowiązujących norm prawa, wkrótce już należeć będzie do przeszłości.

Jak wynika to z art. 79 ust. 1a RODO (które jako rozporządzenie obowiązywać będzie bezpośrednio, bez potrzeby jego implementacji do porządku prawa poszczególnych państw członkowskich), krajowe organy nadzoru zobowiązane będą do nakładania grzywien administracyjnych, mających na celu nie tylko wykonanie nałożonych decyzji nakazowych. Kary te, zgodnie z postanowieniami RODO, mają być skuteczne, proporcjonalne, ale też odstraszające, co zdaje się podkreślać ich represyjny co do zasady charakter. Potwierdzeniem tego jest sam wymiar przewidzianych przez RODO sankcji administracyjnych.

Górna granica kary za naruszenie szczegółowo wskazanych obowiązków administratora (lub innych określonych przez RODO podmiotów) wynieść może nawet 10.000.000 Euro, a w przypadku przedsiębiorcy – do 2% rocznego światowego obrotu w roku poprzedzającym rok naruszenia, w zależności od tego, która z powyższych wartości będzie w danym przypadku wyższa (art. 73 ust. 3-3aa RODO).

Powyższa sankcja odnosi się do takich naruszeń, jak m.in. wdrożenie odpowiednich środków technicznych i organizacyjnych ochrony danych osobowych, odpowiedzialności za rozwiązania stosowane przez tzw. podmiot przetwarzający (w ramach powierzenia przetwarzania danych), czy też brak zgłoszenia przypadków naruszenia bezpieczeństwa danych osobowych. Ogólnie rzecz ujawszy, sankcja ta odnosi się zatem do naruszenia technologicznych i organizacyjnych zasad przetwarzania danych.

Jeszcze poważniejsze – bo sięgające 20.000.000 Euro (lub, w przypadku przedsiębiorców, do 4% rocznego światowego obrotu w roku poprzedzającym naruszenie, w zależności od tego, która z tych wartości okaże się w danym przypadku wyższa) – dotyczą przypadków naruszeń uregulowań RODO wskazanych szczegółowo w art. 79 ust. 3a RODO. Jak wynika z analizy tego przepisu, dotyczy on nie technicznych, a podstawowych zasad postępowania z danymi osobowymi, w tym w szczególności podstaw prawnych przetwarzania danych osobowych (art. 6 RODO), zasady transparentności przetwarzania (art. 5 ust. 1 lit. a) RODO), zasady związania celem przetwarzania (art. 5 ust. 1 lit. b)

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

RODO), czy też zasady tzw. adekwatności – lub minimalizacji przetwarzania danych (art. 5 ust. 1 lit. c) RODO). Sankcja ta odnosi się również m.in. do naruszenia obowiązków informacyjnych i uprawnień podmiotu danych (dotyczących w szczególności dostępu do danych, ich poprawiania, etc.), a także reguł transgranicznego przekazywania danych.

Niezależnie od kar administracyjnych wynikających z samego RODO, państwa członkowskie zobowiązane zostały również do przyjęcia wewnętrznych uregulowań zawierających sankcje prawne dotyczące naruszeń pozostałych uregulowań RODO, które nie zostały objęte zakresem omówionych powyżej artykułów.

Oczywiście omówione wyżej sankcje administracyjne, sięgające nawet kilkudziesięciu milionów Euro, stanowią maksymalny ich wymiar. W konkretnym przypadku ustalenie odpowiedzialności za naruszenie reguł postępowania z danymi osobowymi następować będzie w oparciu o kryteria indywidualizujące określone przykładowo w art. 79 ust. 2a RODO. Rozporządzenie nakazuje zatem brać pod uwagę w szczególności charakter, wagę i czas trwania naruszenia, umyślność lub nieumyślność działania naruszyciela, historię wcześniejszych naruszeń, przebieg współpracy z organem ochrony danych osobowych, a także inne czynniki różnicujące.

Niezależnie od tego, wydaje się, że górna wysokość przewidzianych przez RODO kar administracyjnych może stanowić dla organów zachętę do stosunkowo srogiego ich wymiaru, a nawet kara orzeczona w dolnej granicy zagrożenia (która nie została zdefiniowana), może okazać się niezwykle dotkliwa. Oczywiście weryfikacja tego stanowiska wymagać będzie analizy praktyki GIODO i możliwa będzie dopiero pewien czas po wejściu w życie przepisów RODO.

Mając na uwadze powyższe regulacje, przedsiębiorcy powinni już dziś podjąć odpowiednie działania organizacyjne, które pozwolą zapewnić zgodność prowadzonej działalności z regulacjami z zakresu ochrony danych osobowych.

Koellner Tomasz, aplikant adwokacki Krakowskiej Izby Adwokackiej, prawnik w kancelarii Chabasiewicz Kowalska i Partnerzy.

Absolwent wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego (2011).

Specjalizuje się w prawie własności intelektualnej, prawie nowych technologii, zwalczaniu nieuczciwej konkurencji oraz ochronie danych osobowych.

Autor publikacji z zakresu prawa własności intelektualnej, w szczególności prawa autorskiego. Posługuje się biegle językami angielskim i hiszpańskim.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

dr Lubasz Dominik, radca prawny
LUBASZ I WSPÓLNICY KANCELARIA RADCÓW PRAWNYCH SP.K.

Przesłanki legalizacyjne przetwarzania danych osobowych

Rozporządzenie ogólne[4] **podobnie jak dotychczas obowiązująca dyrektywa 95/46/WE,** przewi**duje dwa reżimy dopuszczalności przetwarzania danych, w zależności od tego, czy poddane mają być temu dane zwykłe czy wrażliwe (szczególne kategorie danych) i zachowuje obowiązujące zasady, tj. ogólnego dopuszczenia przetwarzania danych zwykłych, gdy spełni**ona **jest co najmniej jedna z przesłanek oraz ogólnego zakazu przetwarzania danych wrażliwych, chyba że zachodzi którykolwiek z wyjątków.**

Rozporządzenie ogólne przewiduje w art. 6 zamknięty katalog autonomicznych przesłanek przetwarzania danych zwykłych, do których zaliczane są:

a) zgoda osoby, której dane dotyczą obejmująca przetwarzanie w jednym lub większej liczbie celów;
b) niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na wniosek tej osoby przed zawarciem umowy;
c) niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
e) niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) niezbędność przetwarzania do celów wynikających z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem[5].

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1).
[5] Jako przykłady usprawiedliwionych interesów wskazane zostały w motywach 47-49 rozporządzenia ogólnego m.in. marketing bezpośredni, zapobieganie oszustwom, przekazywanie w ramach grupy kapitałowej, zapewnienie bezpieczeństwa sieci i informacji oraz bezpieczeństwa usług

Gdy przetwarzanie danych oparte jest na przesłance zgody, ciężar udowodnienia istnienia zgody spoczywa na administratorze danych[6]. Zapytanie o zgodę, jeżeli składane jest pisemnie w oświadczeniu dotyczącym także innych kwestii, musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Zgoda może być odwołana w każdym czasie, jej wycofanie nie wpływa na zgodność z prawem przetwarzania dokonywanego do chwili jej wycofania. Odwołanie zgody musi być równie łatwe, jak jej udzielenie.

W sytuacji, w której przetwarzanie danych odbywa się na podstawie zgody i dotyczy usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku poniżej 16 roku życia[7], wymagana jest zgoda od osoby sprawującej władzę rodzicielską. Administrator danych, uwzględniając dostępną technologię ma obowiązek podejmować racjonalne starania, by zweryfikować, czy odpowiednia osoba udzieliła zgody.

Rozporządzenie zachowuje znany dotychczas model zaostrzenia rygoru przetwarzania danych wrażliwych. Zgodnie z art. 9 ust. 1 zasadą jest zakaz przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby lub danych dotyczących zdrowia lub seksualności i orientacji seksualnej, a także danych o wyrokach skazujących i o przestępstwach. Możliwość przetwarzania takich danych dopuszczona jest, gdy spełniono co najmniej jeden z enumeratywnie wymienionych wyjątków:

a) wyraźna zgoda osoby, której dane dotyczą na przetwarzanie danych osobowych w jednym lub kilku konkretnych celach - prawo unijne lub krajowe mogą wyłączyć możliwość uchylenia zakazu przetwarzania opisywanych danych przez sam podmiot danych;
b) niezbędność przetwarzania do wypełnienia obowiązków i skorzystania ze szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony społecznej, o ile jest to dozwolone prawem Unii lub prawem krajowym, lub umową zbiorową na mocy prawa krajowego przewidującymi odpowiednią ochronę praw podstawowych i interesów osoby, której dane dotyczą
c) niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody;

[6] O warunkach udzielania zgody i możliwościach jej wycofania stanowi art. 7 rozporządzenia ogólnego;
[7] Prawo krajowe może przewidywać niższą granicę wieku niż 16 rok życia. Granica ta nie może być jednak niższa niż 13 lat.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

d) przetwarzanie danych przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych w ramach uprawnionej działalności takiego podmiotu, prowadzonej z zachowaniem odpowiednich gwarancji i pod warunkiem, że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane nie są ujawniane poza tym podmiotem bez zgody osób, których dotyczą;
e) okoliczność, że dane zostały podane do wiadomości publicznej w sposób wyraźny przez osobę, której dotyczą;
f) niezbędność przetwarzania do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
g) niezbędność przetwarzania ze względów związanych z ważnym interesem publicznym, na podstawie prawa UE lub prawa krajowego – względy te muszą być proporcjonalne do wyznaczonego celu, nie mogą naruszać istoty prawa do ochrony danych. Muszą również istnieć odpowiedni i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
h) niezbędność przetwarzania do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub społecznej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub społecznej na podstawie prawa Unii lub prawa krajowego lub zgodnie z umową z pracownikiem służby zdrowia;
i) niezbędność przetwarzania ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa krajowego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osoób, których dane dotyczą, w szczególności tajemnicę służbową;
j) niezbędność przetwarzania do celów archiwizacyjnych w interesie publicznym, do celów badań naukowych i historycznych lub do celów statystycznych na podstawie prawa Unii lub prawa krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Nie przewidziano wymogu uzyskania przez administratora pisemnej zgody na przetwarzanie danych szczególnych kategorii.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

O ostatecznym kształcie omawianych przesłanek w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia zdecydują państwa członkowskie, którym w art. 9 ust. 4 rozporządzenia ogólnego przyznano prawo do wprowadzenia dalej idących przesłanek przetwarzania w/w kategorii danych.

Lubasz Dominik, Doktor nauk prawnych, radca prawny, partner zarządzający w Lubasz i Wspólnicy – Kancelaria Radców Prawnych.

Specjalizuje się w prawie nowych technologii, e-commerce, własności intelektualnej, ochronie danych osobowych oraz w prawie gospodarczym, w tym europejskim prawie gospodarczym. Autor licznych publikacji z zakresu ochrony danych osobowych oraz handlu elektronicznego, w tym komentarzy do ustaw, a także cyklicznych artykułów na portalach tematycznych www.PortalPrawaIT.com i www.PortalODO.com, prowadzonych przez ekspertów Kancelarii Lubasz i Wspólnicy.

Ekspert Stowarzyszenia Konsumentów Polskich ds. handlu elektronicznego. Członek Rady Programowej Centrum Ochrony Danych Osobowych i Zarządzania Informacją przy Wydziale Prawa i Administracji Uniwersytetu Łódzkiego

Pękała Michał
DLA PIPER WIATER SP.K.

Koniec dowolności przy profilowaniu danych osobowych

Wykorzystanie mechanizmu profilowania danych jest zjawiskiem powszechnym, szczególnie w Internecie. Usługodawcy z sektora *e-commerce* nierzadko świadczą usługi w postaci dopasowanych do konkretnego użytkownika indywidualnie przygotowanych produktów - zarówno w postaci odpłatnych usług (np. newsletter branżowy), jak również w postaci reklam umieszczanych na stronach internetowych w formie banerów reklamowych (*banner ads*). Obie formy świadczonych usług oparte są na różnych formach profilowania - newsletter bazuje na przedstawionych przez klienta preferencjach, natomiast wyświetlanie konkretnych banerów reklamowych następuje poprzez analizę zachowania użytkownika w Internecie na podstawie plików *cookies*.

Wszystkie formy profilowania łączy wspólny element - wykorzystywanie danych osobowych osób fizycznych. Z przyczyn leżących po stronie tak administracji unijnej, jak również polskiego ustawodawcy, kwestia profilowania przez długi czas nie doczekała się odrębnej regulacji w przepisach dotyczących ochrony danych osobowych. Zwrócić należy jednak uwagę na podejmowane inicjatywy, mające na celu określenie wskazówek dotyczących profilowania, m.in. w formie rekomendacji Rady Europy. Polski organ ds. ochrony danych osobowych (GIODO) również podejmował wysiłki w tym zakresie, zajmując stanowiska w tej kwestii. Żadna z tych inicjatyw nie miała jednak rangi prawa stanowionego i – po mimo iż niezwykle cenne – stanowią one jedynie wskazówki. Sytuacja ta zmieni się wraz z początkiem obowiązywania w połowie 2018 r. uchwalonego przez Parlament Europejski ogólnego rozporządzenia o ochronie danych.

Rozporządzenie wprowadza swoistą rewolucję w dziedzinie ochrony danych osobowych i jest jednocześnie pierwszym aktem prawnym regulującym mechanizm profilowania - i to od razu w skali paneuropejskiej. Zakres zmian obejmuje praktycznie wszystkie aspekty ochrony danych osobowych – od rozszerzenia definicji „danych osobowych", po wprowadzenie ścisłych regulacji dotyczących przetwarzania danych osobowych dzieci. Niniejszy artykuł nie stara się przedstawić wszystkich zmian jakie wprowadza nowe rozporządzenie; celem jego jest zwięzłe omówienie najważniejszych aspektów profilowania na gruncie nowych przepisów.

CZYM JEST PROFILOWANIE?

Rozporządzenie wprowadza szeroką definicję profilowania. Zgodnie z nią, profilowanie stanowi dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu tychże danych do oceny pewnych czynników osobowych osoby fizycznej, np. w formie analizy sytuacji ekonomicznej, zachowania, osobistych preferencji, zainteresowań, wiarygodności czy lokalizacji. Tak pojemna definicja może sprawić, że za profilowanie uznane zostaną czynności powszechne dla aktywności internetowej, np. oferowanie klientom e-sklepów towarów dopasowanych do ich zainteresowań lub dotychczasowych zakupów, bądź dopasowywanie graczy w rozgrywkach wieloosobowych pod względem umiejętności.

NOWE OBOWIĄZKI ADMINISTRATORA DANYCH

Podmioty, które w swojej działalności będą korzystały z profilowania, obowiązane są na gruncie nowej regulacji prawnej do spełnienia – oprócz obowiązków wspólnych dla wszystkich przetwarzających dane – dodatkowych wymogów zarezerwowanych dla tej formy przetwarzania. Obowiązkiem administratora danych, który profiluje (lub zamierza profilować), jest przede wszystkim poinformowanie o tym fakcie osób fizycznych objętych profilowaniem. Co więcej, administrator zobowiązany jest poinformować o zasadach profilowania, jego znaczeniu oraz przewidywanych konsekwencjach dla jednostek. Obowiązek ten uniemożliwia lub znacząco ogranicza profilowanie użytkowników w sposób ukryty.

Zasadą, przyjętą na gruncie rozporządzenia, jest nie podleganie przez osobę fizyczną decyzjom, które zapadły wyłącznie na podstawie zautomatyzowanego przetwarzania danych, w tym w oparciu o operacje profilowania. Rozporządzenie dopuszcza pewne odstępstwa od tej reguły, obejmujące trzy sytuacje:

1. profilowanie jest niezbędne do zawarcia lub wykonania umowy pomiędzy podmiotem danych i administratorem,
2. profilowanie jest wprost przewidziane prawem,
3. jest ono oparte na wyraźnej zgodzie osoby fizycznej

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Dodatkowo, w takich przypadkach administrator zobowiązany jest wdrożyć odpowiednie środki ochrony praw i wolności osoby fizycznej, której danej przetwarzane są w taki sposób. Obejmują one uprawnienie podmiotu danych do uzyskania interwencji ludzkiej ze strony administratora oraz do wyrażenia własnego stanowiska i zakwestionowania tak podjętej decyzji. Istotnym aspektem profilowania, podejmowanego w celach marketingu, jest prawo podmiotu danych do wniesienia – w dowolnym momencie – sprzeciwu. Wskutek sprzeciwu administrator zobowiązany jest do zaprzestania tego rodzaju działań. Dodatkowo, podmiot profilujący użytkowników zobowiązany jest najpóźniej podczas pierwszej komunikacji z osobą, do poinformowaniu o prawie do sprzeciwu wobec profilowania, przy czym informacja taka musi być przedstawiona w sposób jasny i odrębnie od innych informacji zawartych w komunikacie.

W kontekście profilowania należy ponadto wskazać na zmiany jakie wprowadzono w zakresie przesłanek (podstaw) przetwarzania, a szczególnie w zakresie przesłanki zgody. Na gruncie nowej regulacji zgoda musi być m.in. wyrażona w sposób skonkretyzowany, dobrowolny, nie można od niej uzależniać wykonania umowy jeżeli nie jest to konieczne, musi być ona oddzielona od innych kwestii (klauzul) oraz może być ona wycofana w dowolnym momencie. Dodatkowe wymogi przewidziano w zakresie uzyskania zgody dla przetwarzania danych osobowych dzieci.

PROFILOWAĆ?

Nowe rozporządzenie wprowadza daleko idące zmiany. Szereg dodatkowych obowiązków nakładanych na administratora w związku z profilowaniem bez wątpienia zmusi do co najmniej zastanowienia nad tym w jaki sposób ja – administrator – profiluję swoich użytkowników lub klientów. Czasu na dostosowanie się do nowych regulacji jest wystarczająco pod warunkiem, że zmiany nie zostaną zostawione na ostatnią chwilę – wtedy może okazać się, że wraz z początkiem obowiązywania rozporządzenia (25 maja 2018 r.), administrator profiluje dane osobowe niezgodnie z przepisami, co w połączeniu z wprowadzonym katalogiem kar sięgających 20.000.000 EURO może okazać się niezwykle dotkliwe.

Aby odpowiednio przygotować się do profilowania po wejściu w życie nowych przepisów należy przeprowadzić przynajmniej wewnętrzny audyt przetwarzania danych osobowych, uwzględniający m.in. podstawę prawną profilowania danych oraz analizę środków zapewniających ochronę danych. Bardzo pomocne okaże się również z pewnością opracowanie kompleksowej polityki przetwarzania danych osobowych na potrzeby profilowania.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Michał Pękała, LL.M. - prawnik w kancelarii DLA Piper Wiater sp.k. specjalizuje się w zakresie prawa IT, ochrony danych osobowych, a także w zakresie prawa autorskiego. Asystował przy sporządzaniu analiz z zakresu danych osobowych, w tym danych biometrycznych, a także przy optymalizacji data flow dla podmiotów bankowych. Wielokrotnie doradzał również w zakresie prawa autorskiego, w tym w zakresie sporządzania projektów umów dotyczących wdrażania, obsługi oraz utrzymywania systemów IT, umów licencyjnych, klauzul IP w umowach pracowniczych i umowach cywilnoprawnych, umowach o przygotowanie utworów architektonicznych, kwestiach przeniesienia praw majątkowych do utworów. Michał posiada również doświadczenie w obszarze oceny praw własności intelektualnej innowacyjnych start-up'ów, w szczególności na potrzeby otrzymywania dofinansowania ze środków unijnych.
Michał jest ponadto współautorem raportu nt. barier dla innowacyjności w Polsce, przygotowanego na zlecenie Ministerstwa Infrastruktury i Rozwoju.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 **E** BIURO@ECOMMERCEPOLSKA.PL **I** WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA **NIP** 701-039-19-22 **KRS** 0000474028

Tobiczyk Paweł
DLA PIPER WIATER SP.K.

Zasada rozliczalności - nowe wyzwanie dla branży

Przyjęte przez organy unijne rozporządzenie o ochronie danych zastąpić ma w zasadniczej części obowiązującą obecnie krajową ustawę o ochronie danych osobowych. Nowa regulacja zacznie obowiązywać po 2 latach od wejścia w życie, a zatem prawdopodobnie w połowie 2018 roku. Biorąc jednak pod uwagę skalę zmian wynikających z Rozporządzenia, które wprowadza zupełnie nowe lub istotnie zmodyfikowane instytucje i mechanizmy, dotyczące także przetwarzania danych osobowych przez podmioty prowadzące działalność w Internecie, konieczne jest już obecnie rozpoczęcie dostosowania prowadzonej działalności do nowych wymogów. Jest to o tyle istotne, że na gruncie rozporządzenia wzmocniono uprawnienia organów nadzorczych (w tym GIODO), które w przypadku uchybienia obowiązkom będą mogły nakładać na administratorów danych oraz podmioty przetwarzające dane na zlecenie (tzw. procesorów danych) kary finansowe.

Jedną z kluczowych zmian, która będzie miała istotny wpływ również na działalność sklepów internetowych, jest wprowadzenie nieznanej dotąd ustawodawstwu unijnemu oraz krajowemu tzw. zasady rozliczalności (ang. accountability). Zasada ta składa się z dwóch zasadniczych elementów. Po pierwsze, nakłada ona na administratora (np. przedsiębiorcę prowadzącego e-sklep) obowiązek wdrożenia i przestrzegania odpowiednich i skutecznych środków w celu zapewnienia, że przestrzegane są obowiązki prawne w zakresie ochrony danych. Po drugie, zasada ta wymaga, aby podmiot zobowiązany był w stanie wykazać (zademonstrować) zgodność z tymi obowiązkami. Może to zostać zrealizowane za pomocą różnych instrumentów, np. wewnętrznych oraz zewnętrznych polityk prywatności, procedur oraz innego rodzaju dokumentacji, programu szkoleń dla pracowników, zewnętrznych lub wewnętrznych audytów i przeglądów zgodności, certyfikatów, itd.

Zasada rozliczalności ma na celu zapewnienie, aby ochrona danych przeszła niejako z poziomu teorii do praktyki, poprzez wdrożenie mechanizmów pozwalających na wykazanie, że wymagany poziom ochrony danych został zapewniony. Zasada ta jest przykładem regulacji opartej na ryzyku (ang. risk-based regulation), co oznacza, że nie wymaga ona od organizacji podejmowania identycznych środków w każdej sytuacji, lecz pozwala na ich dostosowanie w zależności od poziomu ryzyka związanego z przetwarzaniem danych. W związku z tym, w celu realizacji zasady rozliczalności wszelkie wewnętrzne regulacje e-sklepu (procedury, polityki itp.) powinny uwzględniać w szczególności zakres oraz sposoby przetwarzania danych (operacje na danych) w ramach prowadzonej działalności.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Co ciekawe, obecnie obowiązująca krajowa regulacja z zakresu ochrony danych osobowych przewiduje, w niewielkim zakresie, obowiązki zbliżone do tych wynikających z zasady rozliczalności. Można tu wskazać np. obowiązek opracowania i wdrożenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, które podlegają kontroli GIODO. Nowe przepisy wprowadzają jednak szereg dodatkowych instytucji oraz instrumentów w tym zakresie. Podmioty przetwarzające dane będą zmuszone wkomponować w bieżące procesy biznesowe i kulturę organizacji szereg organizacyjnych oraz technicznych środków ochrony danych. W związku z tym konieczne będzie podjęcie przez przedsiębiorstwa takich działań jak m.in.:

- w określonych w rozporządzeniu przypadkach opracowanie oraz wdrożenie odpowiedniej wewnętrznej dokumentacji (m.in. rejestru czynności przetwarzania danych osobowych, zawierającego takie informacje jak np. cele przetwarzania danych, opis kategorii osób, których dane dotyczą, kategorie odbiorców, którym dane osobowe mogą zostać ujawnione, itp.);
- przedsięwzięcie środków wzmacniających świadomość w zakresie ochrony danych osobowych w organizacji, m.in. poprzez prowadzenie wewnętrznych szkoleń dla pracowników, wdrożenie programów e-learning'owych, itd.;
- przestrzeganie zasady ochrony danych w fazie projektowania (ang. privacy by design) polegającej na uwzględnianiu zasad ochrony danych już na etapie planowania nowych technologii, produktów, usług czy systemów (np. w trakcie planowania oraz przygotowywania nowych rozwiązań i funkcjonalności dostępnych w ramach e-sklepu, wdrażania nowych kampanii marketingowych, itp.);
- uwzględnienie zasady ochrony danych w sposób domyślny (ang. privacy by default), która wymaga, aby ochrona prywatności przyjmowana była jako opcja domyślna, a więc np. aby klient e-sklepu nie był zobowiązany do podejmowania jakichkolwiek dodatkowych działań w celu zabezpieczenia własnych danych ujawnianych w związku z dokonywaniem zakupu czy korzystaniem z innych funkcjonalności, w szczególności w serwisach społecznościowych;
- wyznaczenie - w pewnych przypadkach, np. gdy główna działalność podmiotu przetwarzającego dane wymaga regularnego, systematycznego i prowadzonego na dużą skalę monitorowania osób - inspektora ochrony danych (ang. Data Protection Officer/DPO), tj. osoby dedykowanej w ramach organizacji problematyce ochrony danych.

W tym kontekście należy również wskazać na przewidziany przez rozporządzenie obowiązek przeprowadzenia oceny wpływu procesów przetwarzania danych na prywatność (ang. Privacy Impact Assessment). Rozwiązanie to polega na dokonaniu - jeszcze na etapie poprzedzającym rozpoczęcie

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

przetwarzania danych - oceny skutków planowanych operacji dla ochrony danych. Celem takiej oceny jest określenie procesów przetwarzania danych w organizacji oraz ich wpływu na prywatność, a także zidentyfikowanie, jakie konkretne środki ochrony danych należy wdrożyć w celu realizacji prawnych obowiązków, w tym zasady rozliczalności. Należy przy tym uwzględnić m.in. charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyka związane z ich przetwarzaniem.

Istotne praktyczne znaczenie dla podmiotów prowadzących działalność w Internecie może mieć również przewidziane w rozporządzeniu rozwiązanie dotyczące możliwości poddania się przez podmioty zobowiązane procesowi certyfikacji. Na gruncie nowych przepisów dopuszczalne będzie ustanawianie mechanizmów certyfikacji oraz nadawania specjalnych pieczęci i oznaczeń (w tym paneuropejskich) potwierdzających spełnienie przez organizację wymagań w zakresie ochrony danych osobowych. Certyfikacji dokonywać będą odpowiednie podmioty certyfikujące lub właściwe organy nadzoru na podstawie przyjętej procedury. Mechanizm ten będzie zbliżony do instrumentów, które funkcjonują obecnie w odniesieniu do innych wymogów prawnych - jako przykład można tu wskazać certyfikaty, jakie uzyskać mogą e-sklepy w zakresie zgodności prowadzonej działalności z przepisami z zakresu prawa konsumenckiego. Rozporządzenie przewiduje, że uzyskanie certyfikatu będzie pozwalało na pełniejszą realizację zasady rozliczalności. Jest to więc dodatkowy argument - poza aspektem *stricte* wizerunkowym - przemawiający za zasadnością korzystania przez podmioty prowadzące sklepy internetowe z procedury certyfikacyjnej.

Tobiczyk **Paweł** - aplikant adwokacki, doktorant w Katedrze Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego, pracownik departamentu Intellectual Property and Technology (IPT) w kancelarii prawnej DLA Piper Wiater.

Wiński Marek, radca prawny
KANCELARIA RADCY PRAWNEGO MAREK WIŃSKI

Co dotyczy Unii zostaje w Unii, czyli jednolity zakres stosowania Ogólnego Rozporządzenia o ochronie danych osobowych w Unii Europejskiej

LEAD

Nowe rozporządzenie unijne w sprawie ochrony danych osobowych[8] budzi żywe emocje przede wszystkim ze względu na perspektywę wysokich kar i sankcji za jego naruszenie. W pierwszej kolejności jednak należy skupić się na fundamentach nowej regulacji, czyli ujednoliceniu systemu prawnego oraz zakresie jego zastosowania na terytorium UE. Jest to kwestia wymagająca szczególnej uwagi przedsiębiorców prowadzących działalność w więcej niż jednym państwie UE, jak również tych którzy działając lokalnie, korzystają z usług przedsiębiorców pochodzących spoza terytorium Unii Europejskiej.

PREHISTORIA CZYLI DYREKTYWA 95/46

Dotychczasowy system ochrony danych osobowych w Unii Europejskiej oparty jest na dyrektywie 95/46/WE. Dyrektywa ta powstała w połowie lat dziewięćdziesiątych XX wieku, w czasach, gdy Internet był w pierwszej fazie rozwoju, a na listach przebojów królowała Nirvana. Przez ostatnich dwadzieścia lat jednak wiele się zmieniło. Twórcom dyrektywy o ochronie danych osobowych nie śniło się zapewne, że dzisiaj w zasięgu każdego przedsiębiorcy internetowego będą tak zaawansowane narzędzia przetwarzania danych, jak śledzenie lub profilowanie użytkowników. Pojawiły się nowe globalne koncerny z państw trzecich (szczególnie USA), operujące danymi osobowymi na ogromną skalę (Google, Facebook). Przetwarzając dane setek milionów Europejczyków, firmy te nie podlegają bezpośrednio przepisom unijnym.

Istotny wpływ na kształt systemu ochrony danych osobowych w UE miał również sam charakter prawny dyrektywy. Dyrektywa unijna bowiem wiąże każde państwo członkowskie w odniesieniu do rezultatu, który ma być osiągnięty, ale pozostawia organom krajowym swobodę wyboru formy i środków do jego uzyskania (tak art. 288 Traktatu o funkcjonowaniu Unii Europejskiej). Dyrektywa zatem nie obowiązuje bezpośrednio, lecz wymaga tzw. implementacji (wdrożenia) w systemie prawa krajowego.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: "Ogólne rozporządzenie o ochronie danych" lub "Rozporządzenie")

Każdy kraj członkowski wdrażał dyrektywę „po swojemu" i stosował swoje przepisy prawa krajowego (por. art. 4 Dyrektywy 95/46). W Polsce dyrektywa została implementowana przepisami obowiązującej Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j.Dz.U.2014.1182). Co prawda większość ustaw obowiązujących na terenie UE jest do siebie bardzo podobna, jednak są pewne rozbieżności. Te różnice przekładają się na duże koszty funkcjonowania firm, które przetwarzają dane osobowe w kilku państwach UE. Jeden podmiot przetwarzający dane osobowe w kilku państwach UE musi bowiem spełnić wymogi kilku odrębnych systemów prawa krajowego.

ROZPORZĄDZENIE CZYLI UJEDNOLICENIE

Jednym z głównych celów reformy prawa ochrony danych osobowych było ujednolicenie zasad ochrony na terytorium całej Unii Europejskiej. Rozporządzenie - w odróżnieniu od dyrektywy - ma zasięg ogólny na terytorium całej Unii, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Rozporządzenie nie wymaga implementacji.

Oznacza to, że z chwilą wejścia w życie rozporządzenia na terenie Unii Europejskiej nastąpi ujednolicenie zasad ochrony danych osobowych. Rozporządzenie upoważnia jednak państwa członkowskie do przyjmowania przepisów szczegółowych w określonych obszarach (np. dane przetwarzane w kontekście zatrudnienia, tajemnica służbowa, niektóre aspekty przetwarzania danych biologicznych), które mogą doprecyzowywać zasady ochrony wynikające z rozporządzenia. Czas pokaże, czy w ramach tych wyjątków, niejako „tylnymi drzwiami", nie dojdzie do wprowadzenia istotnych rozbieżności w regulacjach prawnych poszczególnych państw UE.

DZIAŁASZ W UE - PODLEGASZ PRZEPISOM UE

Dyrektywa 95/46 zakładała, że określone w niej zasady ochrony danych osobowych będą miały zastosowanie do podmiotów, które mają siedzibę na terytorium UE lub korzystają ze środków technicznych przetwarzania danych znajdujących się na terytorium UE.

Jak się miało okazać, było to założenie dosyć krótkowzroczne. W jego rezultacie dane setek milionów Europejczyków zaczęły być przetwarzane przez podmioty z państw trzecich, szczególnie USA (Google, Facebook, Dropbox) bez jakiejkolwiek kontroli ze strony europejskich organów nadzoru przetwarzania danych. Przy tym zasady przetwarzania danych osobowych w USA nie spełniały standardów ochrony danych wynikających z dyrektywy 95/46. Problem ten próbowano rozwiązać z różnym skutkiem, ale ostatecznie bez powodzenia (patrz program Safe Harbour)[9].

[9] Program Safe Harbour został opracowany przez Departament Handlu USA w 2000 r. i określał minimalne wymogi co do przetwarzania danych osobowych. Na podstawie decyzji Komisji Europejskiej z 26 lipca 2000 r. uznano, że podmioty, które przystąpią do programu, będą traktowane jako zapewniające wysoki poziom ochrony. Program działał kilkanaście lat do momentu, gdy na skutek skargi Maxa Schremsa, austriackiego prawnika i aktywisty, Trybunał Sprawiedliwości Unii Europejskiej wyrokiem z dnia 6 października 2015 r. stwierdził, że decyzja

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Powyższe problemy w dużym stopniu rozwiązuje nowe rozporządzenie. Przepisy rozporządzenia będą bowiem miały zastosowanie także wobec podmiotów z siedzibą poza UE, o ile oferują osobom przebywającym w Unii swoje towary lub usługi, lub monitorują ich zachowania. Z jednej strony to rozwiązanie dotyczy takich gigantów jak Google czy Facebook, które przy przetwarzaniu danych osobowych z terytorium UE będą musiały stosować przepisy rozporządzenia. Celem tego rozwiązania jest również wykluczenie prób uciekania spod jurysdykcji UE poprzez korzystanie z serwerów znajdujących się poza terytorium UE.

Zgodnie z art. 3 ust. 2 Rozporządzenia:

Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych podmiotów mających miejsce zamieszkania w Unii przez administratora niemającego siedziby w Unii, gdy przetwarzanie wiąże się z:

a) oferowaniem towarów lub usług takim podmiotom danych w Unii, lub

b) monitorowaniem ich zachowania.

PRZEDSTAWICIEL

Administrator przetwarzający dane użytkowników z terytorium UE niemający siedziby w Unii wyznacza swojego przedstawiciela na terytorium Unii (art. 25 ust. 1 Rozporządzenia). Przedstawicielem może być każda osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w Unii, wyraźnie wyznaczona przez administratora, do której organ nadzorczy lub inny podmiot w Unii mogą się zwrócić - zamiast do administratora - w kwestiach dotyczących obowiązków administratora w zakresie przetwarzania i ochrony danych osobowych (art. 4 pkt. 14 oraz 25 ust. 3 Rozporządzenia).

Obowiązku wyznaczenia przedstawiciela na terytorium Unii nie stosuje się do administratora mającego siedzibę w państwie trzecim, jeśli Komisja Europejska zdecydowała, iż dane państwo trzecie zapewnia odpowiedni poziom ochrony (art. 25 ust. 2 Rozporządzenia). Może to nastąpić np. w formie programu podobnego do Safe Harbour, który wyznaczał warunki, jakie powinny spełniać podmioty pochodzące z USA, aby uznać, że przetwarzanie danych osobowych przez te podmioty spełnia minimalne wymagania unijnego systemu ochrony danych osobowych.

Komisji Europejskiej w sprawie zapewnienia odpowiedniego poziomu ochrony w ramach programu „Bezpieczna Przystań" (Safe Harbour) jest nieważna (sprawa C-362/14). W ten sposób utraciła moc podstawa legalności wymiany danych osobowych z podmiotami z USA. W miejsce tego programu ma wejść w życie nowe rozwiązanie pod nazwą Privacy Shield. Co do jego skuteczności jednak nie ma obecnie jednolitego zdania.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

ONE–STOP–SHOP, CZYLI JEDNO OKIENKO

Istotnym ułatwieniem dla przedsiębiorców prowadzących działalność w więcej niż jednym kraju UE będzie wprowadzenie tzw. One-Stop-Shop, czyli systemu jednego okienka obsługi. Spółki lub grupy przedsiębiorstw oferujące usługi na terenie kilku państw UE będą podlegać jednemu organowi nadzoru ochrony danych osobowych w wybranym państwie UE (np. polskiemu GIODO). W przypadku przetwarzania danych osobowych na terytorium UE w ramach jednej Grupy Przedsiębiorstw (np. grupy kapitałowej) za zarządzanie przetwarzaniem danych osobowych będzie odpowiedzialna „główna jednostka organizacyjna" określona według miejsca, w którym odbywają się główne działania związane z przetwarzaniem danych. Właściwość organu nadzoru będzie zależna od lokalizacji takiej "głównej jednostki organizacyjnej". Wybrany organ nadzoru będzie nadzorować wszystkie działania podległego mu podmiotu lub grupy podmiotów związane z przetwarzaniem danych osobowych w całej UE (artykuły 46-55 Rozporządzenia). Krajowy organ nadzoru współpracuje z innymi krajowymi organami nadzoru oraz ma obowiązek składać roczne sprawozdanie z działalności Komisji Europejskiej oraz Europejskiej Radzie Ochrony Danych.

PODSUMOWANIE

Kwestia przedmiotowego i terytorialnego zakresu stosowania ogólnego rozporządzenia o ochronie danych osobowych (RODO) jest istotna zarówno dla przedsiębiorcy e-commerce prowadzącego działalność w kilku państwach UE, jak i przedsiębiorcy działającego lokalnie, który korzysta z usług przedsiębiorców pochodzących spoza terytorium Unii Europejskiej. W takim przypadku dochodzi do powierzenia przetwarzania danych, które wymaga podjęcia określonych prawem czynności (np. zawarcia stosownej umowy). Konieczne będzie ustalenie, gdzie znajduje się główna jednostka organizacyjna danego przedsiębiorcy, kto jest jego przedstawicielem w zakresie ochrony danych osobowych oraz który organ prowadzi nadzór nad przetwarzaniem danych osobowych tego przedsiębiorcy (One–Stop-Shop).

Wiński Marek, radca prawny, partner zarządzający w Kancelarii Wiński (rok założenia 2005).

Specjalizuje się w prawie własności intelektualnej, prawie nowych technologii, ochronie znaków towarowych i domen internetowych, prawie e-commerce i ochronie danych osobowych.

Absolwent prawa na Uniwersytecie Wrocławskim, aplikacji sądowej przy Sądzie Apelacyjnym we Wrocławiu, aplikacji radcy prawnego w OIRP Wrocław oraz studiów podyplomowych w Centrum Praw Własności Intelektualnej im. H. Grocjusza w Krakowie. Wykładowca prawa E-commerce w Wyższej Szkole Bankowej we Wrocławiu.

Rekomendowany w międzynarodowych rankingach jako specjalista z zakresu sporów patentowych oraz ochrony znaków towarowych w Polsce (IAM Patent 1000, WTR 1000).

Witkowska Katarzyna, prawnik
LUBASZ I WSPÓLNICY KANCELARIA RADCÓW PRAWNYCH SP.K.

Inspektor ochrony danych na gruncie RODO

W trakcie prac nad rozporządzeniem ogólnym wiele uwagi poświęcono zadaniom, pozycji i roli inspektora ochrony danych osobowych, jako osoby zapewniającej fachowe wsparcie dla **administratora danych. Ostateczny kształt przepisów odnoszących się do inspektora ochrony danych nie obiega jednak bardzo od konstrukcji przyjętej w polskiej ustawie o** ochronie danych **osobowych. Rozporządzenie wprowadza jednak kilka nowości, które warto mieć na uwadze.**

Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawę swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[10] (dalej „rozporządzenie ogólne") zakłada, że można wyróżnić grupę administratorów danych, których specyfika działania wymaga wskazania osoby dysponującej fachową wiedzą na temat prawa i praktyk w dziedzinie ochrony danych[11]. Do tej grupy rozporządzenie ogólne zalicza:

1. Organy publiczne (z wyjątkiem sądów w ramach sprawowania przez nie wymiaru sprawiedliwości),
2. Administratorów, których główna działalność polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę,
3. Administratorów, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych[12] oraz danych dotyczących wyroków skazujących i naruszeń prawa.

Dla w/w podmiotów rozporządzenie ogólne w art. 37 ustanawia obowiązek wyznaczenia inspektora ochrony danych (dalej także „DPO" od ang. data protection officer). Pierwsza kategoria administratorów objętych obowiązkiem powołania DPO nie budzi wątpliwości. Co do drugiej i trzeciej kategorii, w motywach rozporządzenia ogólnego wyjaśniono, że przetwarzanie danych osobowych jest

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE z 4.5.2016, L 119/1;
[11] Motyw 97 rozporządzenia ogólnego;
[12] Zgodnie z art. 9 rozporządzenia ogólnego do danych szczególnych kategorii zaliczane są: dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne , przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane generyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby;

główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności[13]. Pozostałe podmioty, niemieszczące się w wyżej wskazanym katalogu, będą miały wybór, czy działać samodzielnie czy też korzystać ze wsparcia DPO.

Inspektor ochrony danych osobowych będzie mógł być wybierany i powoływany spośród personelu administratora danych. Będzie mógł też wykonywać swoje zadania na podstawie umowy o świadczenie usług. W każdym wypadku, na inspektora ochrony danych będzie można wyznaczyć tylko taką osobę, która będzie miała odpowiednie kwalifikacje zawodowe, w szczególności wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania przypisanych DPO przez rozporządzenie ogólne zadań i innych obowiązków nałożonych na niego przez administratora danych. Rozporządzenie ogólne nie przewiduje żadnych precyzyjnych kryteriów, w oparciu o które można by ustalić, czy DPO posiada odpowiednie kompetencje do wykonywania swojej funkcji. Administrator danych dokonując wyboru będzie musiał uwzględnić specyfikę swojej działalności, rodzaj operacji prowadzonych na danych i poziom ochrony wymagany dla przetwarzanych danych osobowych.

Przepisy odnoszące się do statusu inspektora ochrony danych[14] wymagają niezwłocznego i właściwego włączania DPO we wszystkie sprawy dotyczące ochrony danych osobowych. Jest to obowiązek administratora danych, stanowiący zarazem istotną gwarancję prawidłowej realizacji zadań przez inspektora ochrony danych. Poza tym, administrator danych ma wspierać DPO w wykonywaniu przez niego zadań, zapewniając mu w tym celu niezbędne zasoby oraz dostęp do danych i operacji przetwarzania. Inspektor ochrony danych nie może otrzymywać żadnych instrukcji dotyczących wykonywanych przez niego obowiązków. Nie może także podlegać karze ani odwołaniu przez administratora danych z tytułu wykonywania swoich zadań. DPO podlegać ma, jak dziś ABI, najwyższemu kierownictwu.

Rozporządzenie ogólne wskazuje również zadania inspektora ochrony danych, zaliczając do nich:

1. Informowanie samego administratora danych, a także jego pracowników o obowiązkach, które spoczywają na nich na mocy rozporządzenia ogólnego oraz przepisów krajowych i doradzanie im w tej sprawie;
2. Monitorowanie przestrzegania przepisów z zakresu ochrony danych osobowych, w tym podejmowanie działań podnoszących świadomość (m.in. szkoleń) uczestników procesów

[13] Motyw 97 rozporządzenia ogólnego;;
[14] Art. 38 rozporządzenia ogólnego;

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

przetwarzania danych i samego administratora danych, związane z tym audyty czy też podział obowiązków;

3. Wspieranie administratora danych w prowadzeniu oceny skutków dla ochrony danych[15] poprzez udzielanie na jego żądanie zaleceń w tej kwestii, a także monitorowanie wykonywania tego zadania przez administratora danych;
4. Współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego. O powołaniu DPO administrator danych będzie musiał poinformować organ nadzorczy (wskazując dane kontaktowe DPO), co w oczywisty sposób ułatwi organowi komunikację z inspektorem ochrony danych;
5. Pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą. Przepisy rozporządzenia ogólnego stanowią, że osoby, których dane dotyczą będą mogły kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących [16]. Przepis dotyczący tego uprawnienia podmiotów danych znalazł się co prawda w artykule dotyczącym statusu DPO, nie jego zadań, ale z perspektywy inspektora ochrony danych taka funkcja punktu kontaktowego będzie właśnie kolejnym zadaniem. Korzystanie przez osoby, których dane dotyczą z możliwości kontaktu z DPO będzie ułatwione dzięki wprowadzeniu obowiązku publikacji danych kontaktowych inspektora ochrony danych przez administratora danych (dane kontaktowe DPO będą stanowiły element obowiązku informacyjnego[17]).

Administrator danych będzie mógł powierzać inspektorowi ochrony danych także inne zadania, ale tylko pod warunkiem, że nie będą one wywoływały konfliktu interesów. Podstawowa grupa obowiązków DPO wynika wprost z przepisów. Wszystkie dodatkowe zadania nie mogą więc kolidować z ich wykonywaniem.

Wszystkie opisane wyżej zasady wyboru, powoływania i funkcjonowania inspektora ochrony danych u administratora danych odnoszą się również do działalności podmiotu przetwarzającego dane, który w tych samych przypadkach będzie musiał wyznaczyć DPO i u którego DPO będzie funkcjonował na tych samych zasadach.

Status DPO, jego niezależność i pozycja w strukturze administratora danych, a także wymogi kwalifikacyjne nie powinny budzić wątpliwości, ponieważ są zbliżone do tych, przewidzianych w polskiej

[15] Art. 35 rozporządzenia ogólnego;
[16] Art. 38 ust. 4 rozporządzenia ogólnego;
[17] Art. 13 i 14 rozporządzenia ogólnego;

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

ustawie o ochronie danych. Nowością dla administratorów danych będzie natomiast obowiązkowe powoływanie inspektora ochrony danych w pewnych przypadkach. Pojawi się także kilka nowych zadań inspektora ochrony danych wynikających w dużej mierze z nowych obowiązków administratorów danych. Właśnie na tych nowych zadaniach powinni się koncentrować obecni administratorzy bezpieczeństwa informacji, którzy będą w przyszłości pełnić funkcję DPO oraz administratorzy danych, którzy DPO będą chcieli powoływać. Czas do 25 maja 2018 roku jest wystarczający, żeby dobrze przygotować się do wykonywania tych nowych zadań i podjąć decyzję, czy powoływać inspektora ochrony danych.

Witkowska Katarzyna, Doktorantka na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego. Specjalizuje się w prawie ochrony danych osobowych – prowadzi audyty, szkolenia i opracowuje dokumentację. Doradza we wdrożeniu systemu ochrony danych osobowych w spółkach z branży nowych technologii i nieruchomości. Ma doświadczenie w zabezpieczeniu danych osobowych w jednostkach medycznych.

Audytor wewnętrzny SZBI wg ISO/IEC 27001:2013.

Wykładowca na Podyplomowych Studiach Ochrony Danych Osobowych organizowanych na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.

Członek zespołu Centrum Ochrony Danych Osobowych i Zarządzania Informacją działającego na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.

Redaktor naczelny portalodo.com

Zawadzka Natalia, adwokat
LUBASZ I WSPÓLNICY KANCELARIA RADCÓW PRAWNYCH SP.K.

Prawo do bycia zapomnianym na gruncie ogólnego rozporządzenia o ochronie danych osobowych

W pracach nad regulacją ochrony danych osobowych od wielu lat zwraca się uwagę na kwestię „prawa do bycia zapomnianym" (ang. *right to be forgotten*). Podstawą tej koncepcji jest założenie, że jednostka powinna być chroniona przed stygmatyzacją wynikającą z pewnych działań podejmowanych przez nią w przeszłości, których ślady można w łatwy sposób odnaleźć w sieci www. Prawo do bycia zapomn**ianym ma stanowić przejaw realizacji podstawowych praw człowieka, takich jak prawo do prywatności i prawo do ochrony danych osobowych.**

Dotychczas prawo do bycia zapomnianym nie było formalnie uregulowane. Na skutek przełomowego wyroku TSUE w sprawie *Google Spain*, najpopularniejsze wyszukiwarki internetowe udostępniły jednak mechanizmy, które pozwalają na usunięcie z wyników wyszukiwania danych nieprawdziwych, a także „niewłaściwych, niestosownych czy też nadmiernych w stosunku do celów, w jakich są przetwarzane", a także takich, które nie są „zaktualizowane czy też są przechowywane przez czas dłuższy niż jest to konieczne – za wyjątkiem przypadków, w których ich przechowywanie jest konieczne dla celów historycznych, statystycznych czy też naukowych"[18]. W swoim orzeczeniu Trybunał zauważył, że może się zdarzyć, że początkowo zgodne z prawem przetwarzanie prawidłowych danych stanie się wraz z upływem czasu bezprawne; będzie tak, gdy dane nie są już potrzebne do realizacji celów, ze względu na które były gromadzone i przetwarzane. Takie dane, uzyskane w drodze wyszukiwania z użyciem imienia i nazwiska jednostki, należy usunąć z listy wyników wyszukiwania, jeśli jednostka się o to zwróci[19].

Analogiczne zasady stanęły u podstaw regulacji prawa do „bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych osobowych[20]. Przyjęto w szczególności, że każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza rozporządzenie ogólne, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Prawo do „bycia zapomnianym" oznacza

[18] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 13 maja 2014 roku w sprawie Google Spain przeciwko Costeja González, C-131/12, pkt. 92.
[19] Tamże, pkt. 93.
[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE z 4.5.2016, L 119/1, dalej: rozporządzenie ogólne.

w szczególności prawo osoby, której dane dotyczą, do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane:

- jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane,
- jeżeli osoba, której dane dotyczą, cofnęła zgodę,
- jeżeli osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania tych danych,
- jeżeli przetwarzanie danych osobowych nie jest z innego powodu zgodne z rozporządzeniem ogólnym[21].

W powyższych sytuacjach osoba, której dane dotyczą, będzie miała prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator będzie miał obowiązek bez zbędnej zwłoki usunąć te dane. Co więcej, jeżeli administrator upublicznił takie dane osobowe, to – uwzględniając dostępną technologię i koszt realizacji – powinien podjąć rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje[22]. W praktyce będzie to oznaczać, że jeżeli osoba, której dane dotyczą, zwróci się np. do administratora portalu społecznościowego o usunięcie jej nieaktualnych danych, to administrator takiego portalu powinien powiadomić operatorów wyszukiwarek o konieczności usunięcia ich również z wyników wyszukiwania.

Prawo do „bycia zapomnianym" spotykało się niejednokrotnie z krytyką obrońców wolności wypowiedzi, w tym prawa do informacji i było porównywane do „poprawiania historii". W odpowiedzi na te argumenty w rozporządzeniu ogólnym wprowadzono zastrzeżenie, że prawo do „bycia zapomnianym" nie znajdzie zastosowania, jeżeli przetwarzanie danych będzie niezbędne:

- do korzystania z wolności wypowiedzi i informacji,
- do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
- do celów archiwalnych w interesie publicznym,
- do celów badań naukowych lub historycznych, lub do celów statystycznych
- do ustalenia, dochodzenia lub obrony roszczeń[23].

[21] Artykuł 17 ust. 1 rozporządzenia ogólnego.
[22] Artykuł 17 ust. 2 rozporządzenia ogólnego.
[23] Artykuł 17 ust. 3 rozporządzenia ogólnego.

Izba Gospodarki Elektronicznej
T + 48 500 390 172 E BIURO@ECOMMERCEPOLSKA.PL I WWW.ECOMMERCEPOLSKA.PL
A RONDO ONZ 1, 00-124 WARSZAWA NIP 701-039-19-22 KRS 0000474028

Przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych ma jednak podlegać odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą. Takie zabezpieczenia mają opierać się na wdrożeniu środków technicznych i organizacyjnych zapewniających w szczególności poszanowanie zasady minimalizacji danych.

Niezależnie od powyższego, osoba, której dane dotyczą, będzie miała prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe, a także uzupełnienia niekompletnych danych osobowych.

Regulacja zawarta w rozporządzeniu ogólnym nakłada na administratorów danych bardzo szerokie obowiązki i w praktyce może rodzić liczne problemy interpretacyjne. Kwestią sporną niewątpliwie pozostanie odpowiednie wyważenie prawa do „bycia zapomnianym" i wolności wypowiedzi. Po wyroku w sprawie Google Spain operatorzy wyszukiwarek utworzyli specjalne działy prawne, których zadaniem jest ocena zasadności żądania usunięcia danych z wyników wyszukiwania. Być może podobne kroki będą musieli podjąć także inni administratorzy.

Natalia Zawadzka, Adwokat - zajmuje się problematyką prawną e-commerce i prawem nowych technologii. Wspiera liczne sklepy i portale internetowe w ich codziennej pracy. Tworzy dla nich regulaminy, polityki prywatności, a także doradza, jak zgodnie z prawem prowadzić marketing w Internecie i rozwiązywać spory z konsumentami.

Specjalizuje się również w prawie autorskim, cywilnym i gospodarczym, zapewniając przedsiębiorcom ich bieżącą obsługę.

Posiada szerokie doświadczenie w prowadzeniu postępowań cywilnych i karnych, w tym w sprawach karnych - gospodarczych.

Członek Komisji Doskonalenia Zawodowego Izby Adwokackiej w Łodzi.

e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

Izba Gospodarki Elektronicznej
Rondo ONZ 1, X p.
00-124 Warszawa
http://www.ecommercepolska.pl

Izba Gospodarki Elektronicznej
Warszawa, 2016