Rok obowiązywania

interpretacje i dobre praktyki branży reklamy internetowej

iab polska

Warszawa, 2019

RODO

Rok obowiązywania RODO

Włodzimierz Schmidt
Prezes Związku Pracodawców Branży Internetowej IAB Polska

Szanowni Państwo,

oddajemy w Wasze ręce raport podsumowujący pierwszy rok obowiązywania rozporządzenia ogólnego o ochronie danych osobowych, czyli doskonale już wszystkim znanego RODO. Dla branży interaktywnej ostatni rok był wyjątkowo pracowity i trudny, ponieważ RODO wywołało tektoniczne zmiany w wielu obszarach działania firm internetowych. Tak dużej zmiany w prawie, o ogromnych konsekwencjach dla przedsiębiorców, chyba nigdy wcześniej nie doświadczyliśmy.

Dodatkowym elementem utrudniającym przedsiębiorstwom dostosowanie się do przepisów RODO, było wprowadzenie przepisów krajowych w ostatniej chwili. Doceniając ogrom pracy i wysiłek polskiego legislatora, który również stanął przed wyjątkowo trudnym zadaniem, nie można jednak zapominać o utrzymującym się bardzo długo stanie niepewności. Wpłynęło to niewątpliwie na opóźnienia po stronie przedsiębiorców oraz na czasami błędne interpretacje, co w konsekwencji naraziło ich na niepotrzebne ryzyko i koszty.

Polscy przedsiębiorcy internetowi zrzeszeni w IAB Polska zaczęli przygotowania już ponad rok przed datą, kiedy RODO zaczęło obowiązywać, podpisując w marcu 2017 roku z Głównym Inspektorem Ochrony Danych Osobowych panią dr Edytą Bielak-Jomaa porozumienie dotyczące wzmocnienia poziomu ochrony danych osobowych na polskim rynku internetowym oraz upowszechnienia i jednolitego wdrażania zasad tej ochrony zgodnie z europejskimi i polskimi regulacjami prawnymi w tym zakresie. Zawarcie tej umowy było podyktowane jednak przede wszystkim potrzebą efektywnego dostosowania się do RODO.

Wynikiem porozumienia było powstanie w ramach struktur IAB Polska Zespołu Roboczego RODO, w skład którego weszli przedstawiciele zrzeszonych firm wydawców, agencji, domów mediowych, firm technologicznych i kancelarii prawnych. Grono ekspertów liczące kilkadziesiąt osób przez rok pracowało nad wypracowaniem i ujednoliceniem zgodnych z RODO dobrych praktyk rynkowych. Podczas spotkań, wielogodzinnych dyskusji i analiz, gdzie nieraz „zderzały się" przepisy prawa z możliwościami technologicznymi, powstał zbiór dobrych praktyk, któremu nadaliśmy formę „Kodeksu postępowania i dobrych praktyk RODO w branży reklamy internetowej". Liczymy, że po jego zatwierdzeniu przez regulatora stanowić on będzie istotny element *compliance* w działalności podmiotów z sektora reklamy internetowej. Warto w tym miejscu podkreślić wsparcie udzielone w trakcie prac przez organ ds. ochrony danych osobowych, czyli

GIODO, a następnie UODO. W trakcie prac nad kodeksem wspólnie z przedstawicielami UODO organizowaliśmy spotkania i warsztaty, które pomogły obu stronom lepiej zrozumieć nie tylko zawiłości interpretacyjne, ale też możliwości i ograniczenia wynikające z dostępnych na rynku technologii.

Kodeks został szeroko skonsultowany społecznie jeszcze w 2018 roku. W wyniku konsultacji powstał dokument, który jest gotowy do oficjalnego zatwierdzenia przez UODO. Jednak największą dotychczasową korzyścią nie jest samo opracowanie projektu kodeksu, a fakt wypracowania zgodnych z RODO dobrych praktyk rynkowych, szeroko dyskutowanych i analizowanych, a przede wszystkim jednolicie stosowanych przez całą branżę reklamy internetowej.

W oddawanym w Wasze ręce raporcie opisujemy te najważniejsze rozwiązania i dobre praktyki.

Życzę ciekawej i wartościowej lektury.

Włodzimierz Schmidt

Związek Pracodawców Branży Internetowej IAB Polska jest organizacją zrzeszającą ponad 230 najważniejszych firm polskiego rynku internetowego, w tym największe portale internetowe, sieci reklamowe, domy mediowe, agencje interaktywne, firmy technologiczne oraz reklamodawców. Jego głównym celem jest szeroko pojęta edukacja rynku w zakresie wykorzystania internetu jako skutecznego narzędzia prowadzenia biznesu i komunikacji marketingowej. Propaguje skuteczne rozwiązania e-marketingowe i reklamowe oraz tworzy, prezentuje i wdraża branżowe standardy jakościowe. Przygotowuje raporty, badania rynku online i poradniki, m.in. Raport Strategiczny czy AdEx, którego wyniki są bazą analiz wydatków reklamowych. Jest organizatorem konferencji (Forum IAB, IAB HowTo), konkursów (IAB MIXX Awards), warsztatów i szkoleń (np. Akademia DIMAQ). Jednym z flagowych projektów IAB Polska jest DIMAQ – standard kompetencji oraz program certyfikujący wiedzę z dziedziny e-marketingu.

IAB Polska działa od 2000 roku, jest częścią światowych struktur IAB, członkiem IAB Europe oraz IAB Tech Lab, a także Związku Stowarzyszeń Rada Reklamy, Krajowej Izby Gospodarczej i Business Center Club.

www.iab.org.pl

Anna Mazur
menedżer
ds. regulacyjnych
IAB Polska

PRACE ZESPOŁU RODO W IAB POLSKA

Od kilku lat w IAB Polska regularnie działa Grupa Prawna zrzeszająca szefów i członków zespołów prawnych naszych firm członkowskich – wydawców, platform internetowych, agencji interaktywnych i domów mediowych, firm z branży programatycznej, a także firm doradczych i kancelarii prawnych – która stanowi istotne wsparcie dla działań *public affairs* Związku. Jej głównym celem jest uzgadnianie i opracowywanie stanowisk IAB Polska, które prezentują podejście branży do projektów legislacyjnych i pozalegislacyjnych, są także formą dialogu z legislatorami i regulatorami rynku.

Kiedy w 2016 r. zostało przyjęte rozporządzenie ogólne o ochronie danych osobowych w Unii Europejskiej (RODO), okazało się, że działania mające na celu dostosowanie polskiego prawa i działania organów ochrony danych osobowych do nowych wymogów, a co za tym idzie także konieczność dostosowania praktyk biznesowych, będą tak rozległym i absorbującym branżę internetową zadaniem, że z Grupy Prawnej wydzielił się dedykowany Zespół RODO, który zajął się tematem ochrony danych osobowych. Zespół opracowywał stanowiska branży wobec projektów ustaw mających na celu dostosowanie polskiego prawa do RODO[1], a jego przedstawiciele brali udział w wypracowywaniu poradników o RODO w ramach grup roboczych funkcjonujących w Ministerstwie Cyfryzacji[2]. Na arenie europejskiej Zespół uczestniczył projektach pilotowanych przez IAB Europe, tj. przede wszystkim w wypracowywaniu branżowych dokumentów roboczych (*GDPR Compliance Primer, Working Paper on the Definition of Personal Data, Working Paper on GDPR Consent, Working Paper on Data Subject Requests, Working Paper on Controller – Processor Criteria*)[3], opiniowaniu wytycznych wydawanych najpierw przez tzw. Grupę Art. 29, a następnie Europejską Radę Ochrony Danych, a także tworzeniu mechanizmu *Transparency & Consent Framework*[4], czyli branżowych ram służących ustrukturyzowanemu zbieraniu zgód użytkowników.

Kodeks postępowania i dobrych praktyk RODO w branży reklamy internetowej

W toku wymiany poglądów na temat podejścia i sposobów dostosowania swoich praktyk biznesowych do wymogów RODO, Zespół szybko zauważył, że najlepszą gwarancją zgodności i potwierdzeniem wywiązywania się z obowiązków nałożonych w przepisach RODO byłoby opracowanie branżowego kodeksu postępowania, który zostałby przedłożony do zatwierdzenia polskiemu organowi ochrony danych osobowych. Taki mechanizm współregulacji jest przewidziany w przepisach RODO w art. 40. Tak powstał pomysł opracowania kodeksu postępowania i dobrych praktyk RODO dla branży reklamy internetowej, który stał się pierwszoplanowym projektem Zespołu. Jeszcze w 2017 r. Związek Pracodawców Branży Internetowej IAB Polska podpisał z ówczesnym GIODO porozumienie o wspólnym działaniu na rzecz podnoszenia poziomu ochrony danych osobowych w komunikacji interaktywnej i rynku internetowym oraz tworzenia kodeksu postępowania, a następnie ruszyły prace redakcyjne. IAB Polska sukcesywnie dzieliło się postępami prac nad kodeksem z Urzędem Ochrony Danych Osobowych na organizowanych przez regulatora spotkaniach oraz na dwustronnych warsztatach. 22 maja 2018 r. gościliśmy w IAB Polska Pana Dyrektora Piotra Drobka, który wraz z towarzyszącymi mu przedstawicielami UODO prowadził warsztaty, na których dyskutowaliśmy o największych wyzwaniach dostrzeżonych przez branżę podczas prac nad kodeksem. Omówiliśmy kwestie szczególnie istotne dla branży, takie jak: sposoby spełnienia obowiązku informacyjnego w serwisach internetowych, sposoby udzielania zgody, a także kwestie dotyczące realizacji praw podmiotów danych osobowych.

---

[1] https://iab.org.pl/legislacja/stanowiska/stanowisko-iab-polska-dot-projektow-ustaw-dostosowujacych-polskie-prawo-do-rodo/
https://iab.org.pl/legislacja/stanowiska/stanowiski-iab-polska-w-sprawie-art-5-projektu-ustawy-o-ochronie-danych-osobowych/
https://iab.org.pl/legislacja/stanowiska/iab-polska-apeluje-w-sprawie-zmian-wprowadzonych-w-art-18-ust-1-4-usude/

[2] https://www.gov.pl/web/cyfryzacja/przewodnik-po-rodo

[3] https://www.iabeurope.eu/policy/iab-europes-gdpr-compliance-primer/
https://www.iabeurope.eu/policy/gig-working-paper-on-the-definition-of-personal-data/
https://www.iabeurope.eu/policy/gig-working-paper-on-gdpr-consent/
https://www.iabeurope.eu/policy/iab-europe-gig-working-paper-on-data-subject-requests/
https://www.iabeurope.eu/policy/iab-europe-gig-working-paper-on-controller-processor-criteria/

[4] https://advertisingconsent.eu/

1. Warsztaty na temat kodeksu postępowania i dobrych praktyk RODO w branży reklamy internetowej (IAB Polska, 22.05.2018)

Pierwszej prezentacji założeń kodeksu dla szerokiej publiczności – firm z branży interaktywnej – dokonaliśmy na Forum IAB 2018 podczas prezentacji mecenasa Xawerego Konarskiego.

2. Mec. Xawery Konarski podczas wystąpienia na Forum IAB 2018 (Warszawa, 6-7.06.2018)

Konsultacje społeczne Kodeksu RODO

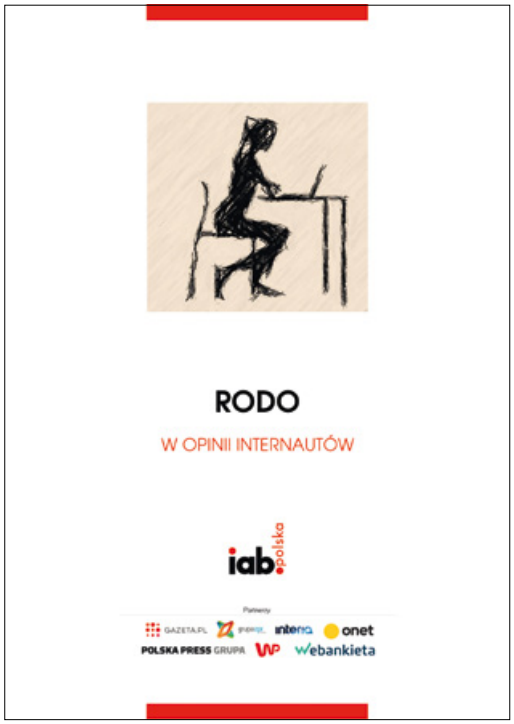
Prace redakcyjne nad projektem kodeksu zostały sfinalizowane latem 2018 i w sierpniu tego samego roku ogłoszone zostały konsultacje publiczne dotyczące projektu kodeksu[5]. Następnie do kodeksu wprowadziliśmy poprawki zgłoszone w formie pisemnej i spotkaliśmy się z najbardziej zainteresowanymi interesariuszami.

Zespół podjął decyzję o przeprowadzeniu badania, które potraktowaliśmy jako dodatkowy instrument – formę bezpośrednich konsultacji z osobami, których dane dotyczą, przewidziany w motywie 99 RODO. Badanie zostało zrealizowane we współpracy z dużymi portalami informacyjnymi oraz sieciami reklamowymi: Gazeta.pl, Grupa ZPR Media, Interia, Onet, Polska Press Grupa, Wirtualna Polska. Dzięki takiemu doborowi próby podczas realizacji projektu rekrutowano internautów na kilku tysiącach zróżnicowanych pod względem profilu witryn, a wspólny zasięg osiągnięty w badaniu wyniósł ponad 95% polskich internautów (na podstawie łącznego zasięgu według badania Gemius/PBI).

Z badania opracowany został raport „RODO w opinii internautów”[6], który z jednej strony pomógł Zespołowi lepiej zrozumieć oczekiwania użytkowników dotyczące wdrożenia różnych rozwiązań wymaganych przez RODO, a także stanowił kontynuację wieloletnich już badań prowadzonych przez IAB Polska w obszarze prywatności (np. raport „Prywatność w sieci 2016/2017”, kampania „Wszystko o ciasteczkach”).

[5] https://iab.org.pl/aktualnosci/iab-polska-uruchamia-konsultacje-projektu-kodeksu-rodo/

[6] https://iab.org.pl/badania-i-publikacje/raport-rodo-w-opinii-internautow-2/



3. Raport „RODO w opinii internautów”

Podczas Konferencji z okazji obchodów XIII Dnia Ochrony Danych Osobowych organizowanej przez UODO w dniu 28.01.2019 r. Marcin Gotkiewicz, Szef Grupy Prawnej IAB Polska z WP oraz Agnieszka Sagan-Jeżowska z Edipresse podzielili się doświadczeniami branży dotyczącymi realizacji praw podmiotów danych w internecie.

4. Konferencja z okazji obchodów XIII Dnia Ochrony Danych Osobowych (Warszawa, 28.01.2019)

22 lutego 2019 roku odbyły się natomiast warsztaty dotyczące reklamy *programmatic* w siedzibie UODO z udziałem pani Minister Edyty Bielak-Jomaa. Było to wydarzenie, które miało na celu przedstawienie modelu reklamy *programmatic* i dyskusję o zidentyfikowanych problemach prawnych dotyczących ochrony danych osobowych w powyższym modelu.

5. Warsztaty dotyczące reklamy *programmatic* (Warszawa, 22.02.2019)

W czerwcu 2019 r. Europejska Rada Ochrony Danych przyjęła ostateczną wersję wytycznych w sprawie kodeksów postępowania. Jak tylko ww. wytyczne zostaną przełożone na grunt polskich przepisów oraz wypracujemy operacyjne mechanizmy monitorowania działań sygnatariuszy, planujemy przedłożyć projekt kodeksu postępowania i dobrych praktyk RODO branży reklamy internetowej do formalnego zatwierdzenia przez Prezesa UODO.

Zakończenie prac nad kodeksem nie jest jednoznaczne z zakończeniem prac Zespołu RODO. Branża internetowa nadal napotyka na problemy interpretacyjne dotyczące przepisów Rozporządzenia, a wspólna dyskusja i wymiana poglądów jest korzystna zarówno dla branży, jak i użytkowników internetu.

Na horyzoncie pojawia się również nowa, bardzo istotna dla reklamy internetowej, regulacja – projekt Rozporządzenia Parlamentu Europejskiego i Rady o e-prywatności, nad którą prace trwają już od 2017 r. Jest to regulacja sektorowa, uzupełniająca RODO w zakresie przetwarzania danych osobowych w sieciach łączności elektronicznej. Zespół RODO IAB Polska od początku monitoruje prace nad tym aktem prawnym i z pewnością będzie brał aktywny udział w wypracowywaniu jego interpretacji.

Xawery Konarski
adwokat,
Traple Konarski Podrecki i Wspólnicy

REKLAMA INTERNETOWA – SYSTEM PRZEPISÓW PRAWNYCH O OCHRONIE DANYCH OSOBOWYCH I PRYWATNOŚCI

Nowe przepisy o ochronie danych osobowych w Unii Europejskiej – RODO i dyrektywa policyjna

Na pakiet normatywny reformujący ochronę danych osobowych w Unii Europejskiej składają się dwa akty prawne:

1) 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, dalej określane jako „RODO" lub „Rozporządzenie") oraz

2) dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW („dyrektywa policyjna").

Przepisy RODO obowiązują od 25 maja 2018 r. Rozporządzenie ma zasięg ogólny, wiąże w całości co do wszystkich zawartych w nim postanowień i jest bezpośrednio stosowane we wszystkich państwach członkowskich, bez potrzeby dokonywania implementacji do przepisów krajowych. Taki charakter przepisów Rozporządzenia związany jest z jednym z podstawowych celów uchwalenia RODO, tj. likwidacji fragmentaryzacji ochrony danych osobowych w poszczególnych państwach Unii Europejskiej i zapewnienia równorzędnego stopnia ochrony na terytorium całej Unii. Przepisy RODO w pełnym zakresie znajdują zastosowanie do podmiotów z branży reklamy internetowej.

Dyrektywa 2016/680 traktowana jest jako uzupełnienie RODO w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. W tym zakresie bowiem RODO wyłącza stosowanie swoich przepisów (tak art. 2 ust. 2 lit. d RODO).

Prawodawca europejski celowo uregulował powyższe kwestie – ze względu na szczególny charakter takich czynności – w akcie prawnym innej rangi, to jest dyrektywie. Dyrektywa bowiem, jako akt prawny zobowiązujący państwa członkowskie do ustanowienia danego porządku prawnego – w przeciwieństwie do rozporządzenia, którego przepisy mają zastosowanie wprost – pozwala na uwzględnienie w przygotowywanych na jej podstawie przepisach odmienności krajowych regulacji w zakresie zapobiegania i zwalczania przestępczości. Przykładem tego rodzaju odmienności w prawie polskim jest chociażby niewystępujące w innych państwach Unii Europejskiej, rozróżnienie czynów karalnych na przestępstwa i wykroczenia. Przepisy Dyrektywy 2016/680 zostały wprowadzone do polskiego porządku prawnego w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125). Weszła ona w życie w dniu 6 maja 2019 r. Z punktu widzenia branży reklamy internetowej jej znaczenie jest marginalne.

Uzupełnienie przepisów RODO na poziomie krajowym – ustawa kompetencyjna i ustawa dostosowująca (przepisy sektorowe)

Niezależnie od bezpośredniej stosowalności przepisów RODO, w Rozporządzeniu przewidziano również w pewnym zakresie jego uzupełnienie przepisami krajowymi. W Polsce uzupełnienie tego rodzaju nastąpiło w dwóch aktach prawnych:

1) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000), tzw. „ustawa kompetencyjna", „uodo", która weszła w życie w dniu 25 maja 2018 r. oraz

2) ustawie z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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 (Dz.U. z 2019 r., poz. 730), tzw. „ustawa dostosowująca", która weszła w życie w dniu 4 maja 2019 r. W przypadku branży internetowej najważniejsze zmiany wprowadzono na jej podstawie w ustawie o świadczeniu usług świadczonych drogą elektroniczną oraz ustawie – Prawo Telekomunikacyjne (odpowiednio art. 63 oraz art. 79 ustawy dostosowującej).

Na całość sytemu przepisów RODO składają się więc nie tylko przepisy Rozporządzenia, ale również wydanych w związku z nim ustaw krajowych. Ma to istotne znaczenie prawne, ponieważ naruszeniem przepisów Rozporządzenia, skutkującym między innymi możliwością nałożenia przez Prezesa Urzędu Ochrony Danych Osobowych wysokich kar pieniężnych jako sankcji administracyjnych (art. 83 RODO), będzie również naruszenie przepisów ustaw krajowych, doprecyzowujących RODO.

Ustawa kompetencyjna – kompetencje organu, odpowiedzialność cywilna i karna, instrumenty *compliance*

W ustawie kompetencyjnej znajdują się przede wszystkim te postanowienia, których przyjęcia w przepisach krajowych wymaga RODO. Do najważniejszych z nich zaliczyć należy określenie sposobu wyboru i kompetencji Prezesa Urzędu Ochrony Danych Osobowych (PUODO) jako organu właściwego w sprawach ochrony danych osobowych (art. 34 i n. uodo) oraz zasad prowadzenia postępowań administracyjnych w sprawie naruszenia przepisów o ochronie danych osobowych (art. 60 i n. uodo). Wiążą się z nimi bezpośrednio przepisy dotyczące postępowania kontrolnego prowadzonego przez PUODO (art. 78 i n. uodo) oraz przesłanek nakładania przez ten organ administracyjnych kar pieniężnych przewidzianych w RODO (art. 101 uodo).

Nowy organ nadzorczy w zakresie ochrony danych osobowych otrzymał istotnie szerszy katalog kompetencji, w głównej mierze zdeterminowany przepisami RODO. Do najistotniejszych obszarów działań PUODO zaliczyć należy:

- prowadzenie ewidencji inspektorów ochrony danych osobowych powołanych przez administratorów (art. 10 uodo),
- opracowanie kryteriów certyfikacji (art. 16 uodo), o której mowa w art. 42 RODO, oraz przeprowadzanie certyfikacji (art. 15 ust. 1 uodo),
- prowadzenie elektronicznego systemu umożliwiającego administratorom zgłaszanie naruszeń ochrony danych osobowych na podstawie art. 33 RODO,
- umożliwienie administratorom uprzednich konsultacji w zakresie operacji, co do których ocena skutków wykazała wysokie ryzyko, o czym mowa w art. 36 RODO,
- prowadzenie postępowań kontrolnych przez upoważnionych pracowników Urzędu zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa informacji (art. 78 i 79 ust. 1 uodo),
- prowadzenie postępowań w sprawie naruszenia przepisów o ochronie danych osobowych oraz nakładanie administracyjnych kar pieniężnych na podstawie art. 83 ust. 2 RODO. Działania w ramach realizacji tego zadania zostały zabezpieczone szeregiem uprawnień dla Prezesa UODO, które mają pomóc w efektywnym podnoszeniu poziomu ochrony danych osobowych (rozdział 7 uodo),

- zatwierdzanie kodeksów postępowań oraz akredytacja podmiotów monitorujących przestrzeganie zatwierdzonych kodeksów, zgodnie z art. 40 RODO (rozdział 5 RODO),
- pełnienie roli organu doradczego i opiniotwórczego w zakresie podnoszenia standardów ochrony danych osobowych, m.in. przez wydawanie rekomendacji.

Odrębne przepisy dotyczą uzupełnienia postanowień RODO odnośnie odpowiedzialności cywilnoprawnej z tytułu naruszenia przepisów o ochronie danych osobowych oraz związanych z tym proceduralnych zagadnień dochodzenia roszczeń przed sądami powszechnymi (art. 92 i n. uodo). W ustawie kompetencyjnej wprowadzono również przepisy karne za bezprawne przetwarzanie danych osobowych oraz za utrudnianie prowadzenia kontroli przez PUODO (art. 107-108 uodo).

Nowym, w stosunku do dotychczasowego stanu prawnego, rozwiązaniem przewidzianym w RODO jest możliwość wykazywania przez podmioty przetwarzające dane osobowe zgodności z wymogami Rozporządzenia poprzez stosowanie określonych w nim instrumentów *compliance* (m.in. kodeks postępowania oraz mechanizmy certyfikacji). W związku z tym w ustawie kompetencyjnej znalazły się przepisy określające warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych („podmiot certyfikujący"), akredytowanego przez Polskie Centrum Akredytacji, oraz trybu dokonywania samej certyfikacji (art. 15 i n. uodo). Podobny charakter mają postanowienia o trybie zatwierdzenia kodeksu postępowania oraz podmiocie monitorującym kodeks postępowania (art. 27 i n. uodo).

Ustawa dostosowująca do RODO – przepisy sektorowe branży internetowej

Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO zawiera nowelizacje ponad 160 ustaw. W przypadku branży internetowej najważniejsze zmiany wprowadzono w ustawie o świadczeniu usług drogą elektroniczną („uśude") oraz ustawie – Prawo Telekomunikacyjne („PT").

Zmiany w uśude – nowe zasady przetwarzania danych eksploatacyjnych

Zmiany wprowadzone w ustawie o świadczeniu usług drogą elektroniczną w pierwszej kolejności potwierdzają zasadę, że zgoda usługobiorcy powinna być pozyskiwana na takich zasadach, jak to określono w przepisach o ochronie danych osobowych, tj. RODO (art. 4 uśude). Odwołanie to oznacza, iż dla skutecznego pozyskania zgody na przetwarzanie danych osobowych w związku ze świadczeniem usług drogą elektroniczną konieczne jest w szczególności spełnienie warunków określonych w art. 4 ust. 11, art. 7 oraz art. 8 RODO.

Istotnej zmianie uległ dotychczasowy rozdział IV uśude pt. „Zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną" (art. 16-22). Z uwagi na bezpośrednie stosowanie RODO uchylono bowiem większość zawartych w nim przepisów, tj. art. 16-17, 19 ust. 1-2 i 4-5 oraz art. 20-22 uśude. Legalność przetwarzania danych osobowych w sytuacjach opisanych w tych przepisach oceniana jest więc obecnie na podstawie właściwych przepisów RODO.

W treści rozdziału IV pozostawiono natomiast dwie kategorie przepisów:
- implementujące dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz
- regulacje nienaruszające RODO i nieobjęte jego treścią.

Do pierwszej grupy przepisów zaliczyć należy art. 18 ust. 4 uśude, który po jego nowelizacji brzmi następująco: „Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną". Znowelizowana treść tego przepisu budzi istotne kontrowersje interpretacyjne. Zgodnie bowiem z jego literalną treścią usługodawcy zobowiązani są do pozyskiwania zgody użytkownika (usługobiorcy) na przetwarzanie jego danych osobowych, innych niż niezbędne do świadczenia usług drogą elektroniczną, (np. informacje o odwiedzanych przez nich stronach internetowych). Dotyczy to między innymi sytuacji, gdy dochodzi do przetwarzania tych danych na cele marketingowe czy analityczne. Stanowi to istotną zmianę w stosunku do dotychczasowego stanu prawnego, w którym obowiązek pozyskania takiej zgody aktualizował się dopiero po „zakończeniu korzystania z usługi świadczonej drogą elektroniczną", a nie w trakcie jej świadczenia (uchylony art. 19 ust. 2 uśude).

Do drugiej grupy przepisów pozostawionych w rozdziale IV uśude zaliczyć należy art. 18 ust. 6 uśude, nakładający na usługodawców obowiązek nieodpłatnego udostępniania danych organom państwa, uprawnionym na podstawie odrębnych przepisów, na potrzeby prowadzonych przez nie postępowań oraz art. 19 ust. 3 uśude, zgodnie z którym „Rozliczenie usługi świadczonej drogą elektroniczną przedstawione usługobiorcy nie może ujawniać rodzaju, czasu trwania, częstotliwości i innych parametrów technicznych poszczególnych usług, z których skorzystał usługobiorca, chyba że zażądał on szczegółowych informacji w tym zakresie".

Zmiany w PT – konsekwencje dla korzystania z *cookies* reklamowych

Z punktu widzenia branży reklamy internetowej, najważniejsze zmiany wprowadzone ustawą dostosowującą w Prawie Telekomunikacyjnym dotyczą przepisów o zgodzie abonenta lub użytkownika. W znowelizowanym PT przyjęto, podobnie jak w uśude, zasadę, że zgoda abonenta lub użytkownika końcowego powinna być pozyskana na takich zasadach, jak to określono w przepisach o ochronie danych osobowych, tj. RODO (art. 174 PT).

Cookies jako dane osobowe

Zmiana wprowadzona w art. 174 PT jest między innymi konsekwencją uznania *cookies* (ciasteczka) za dane osobowe. Zgodnie bowiem z definicją legalną „danych osobowych" (art. 4 pkt 1 RODO), pojęcie to obejmuje identyfikatory internetowe. Dalszych wskazówek interpretacyjnych w tym względzie należy doszukiwać się w motywie 30 RODO, zgodnie z którym „osobom fizycznym mogą

zostać przypisane **identyfikatory internetowe** – takie jak adresy IP, identyfikatory plików *cookie*[7] – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane np. przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób".

W świetle powyższego, **na gruncie RODO należy przyjąć, że identyfikatory *cookies* w zdecydowanej większości przypadków powinny być traktowane jako dane osobowe**. Przesądza o tym okoliczność ich przypisania do urządzenia (*cookies ID*), z czym wiąże się potencjalna możliwość identyfikacji danej osoby fizycznej, względnie możliwość traktowania informacji o tej osobie jako „unikalnej", nawet jeżeli nie jest możliwa jej bezpośrednia identyfikacja. Tę „unikalność" należy bowiem rozumieć jako możliwość wyodrębnienia informacji o danej osobie. Potwierdza to jednoznacznie motyw 26 RODO, zgodnie z którym: „(…) Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej".

W podsumowaniu powyższego należy stwierdzić, że używanie ciasteczek w celu „śledzenia" aktywności danej osoby w sieci stanowić będzie przetwarzanie danych osobowych, o ile takie „śledzenie" wiązać się będzie z korzystaniem z identyfikatora internetowego, który jest użyty do tworzenia profilu tej osoby. Nie jest przy tym konieczne, aby unikalne *cookie ID* było łączone z informacjami bezpośrednio identyfikującymi daną osobę (np. jej nazwiskiem, adresem poczty elektronicznej itp.). Kwalifikacji tej nie zmienia również spseudonimizowany charakter informacji zawartych w identyfikatorach, a które to stanowią ciąg liczb lub liter. Na gruncie rozporządzenia 2016/679 informacje tego rodzaju powinny być bowiem również traktowane jako dane osobowe[8].

Warunki dopuszczalnego korzystania z *cookies* reklamowych

Zasady korzystania z *cookies* mających charakter danych osobowych w rozumieniu RODO, określone są w PT. Z punktu widzenia stosowania zasad dopuszczalnego korzystania, ciasteczka należy podzielić na tzw. *essential* oraz *non-essential cookies*. Ciasteczka „niezbędne" (*essential*) to takie, które są konieczne do prawidłowego działania odwiedzanej strony internetowej i jej podstawowych funkcji. Bez nich określona strona internetowa nie mogłaby wypełnić swojego podstawowego zadania. Korzystanie z nich odbywa się na podstawie przepisów prawa (art. 173 ust. 3 pkt 1-2 PT). W przypadku innych ciasteczek (np. *cookies* reklamowych), legalność ich wykorzystywania wymaga bezpośredniego poinformowania abonenta (użytkownika) o celach i najważniejszych konsekwencjach instalowania i odczytywania informacji zawartych w ciasteczkach, a także uzyskania uprzedniej, a więc jeszcze przed podjęciem tych czynności, zgody na ich dokonanie.

Dla przyjęcia, iż zgody na *cookies* reklamowe są skutecznie udzielane, w istocie konieczne jest więc **łączne spełnienie trzech warunków**.

Po pierwsze, zamieszczanie ciasteczek nie może rozpocząć się przed wyrażeniem zgody przez użytkownika. W przypadku stron internetowych, wymóg ten może zostać spełniony m.in. przez stosowanie tzw. „stron pośrednich" (*interstitial sites*), poprzez które odbywa się zapytanie o wyrażenie zgody. Na stronach tych powinna być zablokowana możliwość instalowania ciasteczek (*consent-wall*).

Po drugie, użytkownikowi powinny zostać podane uprzednio informacje określone w przepisach RODO oraz PT. W przypadku PT, z uwagi na wyraźne brzmienie art. 173 ust. 1 pkt 1 PT, informacje te powinny zostać przekazane bezpośrednio na stronie internetowej.

[7] Motyw 30 RODO jest jedynym miejscem w rozporządzeniu 2016/679, w którym następuje bezpośrednie odwołanie się do ciasteczek.

[8] Motyw 26 RODO.

Po trzecie, konieczna jest jakaś forma aktywności podmiotu danych (użytkownika). Istotnej wskazówki interpretacyjnej dostarcza nam motyw 32 RODO, w którym wskazano przykłady sytuacji, które stanowią (lub nie) „wyraźne działanie potwierdzające": „Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody". W świetle treści motywu 32 RODO nie budzi wątpliwości, że samo kontynuowanie zwykłego korzystania ze strony internetowej nie jest zachowaniem, na podstawie którego można wywnioskować złożenie przez osobę, której dane dotyczą, oświadczenia woli polegającego na wyrażeniu zgody na proponowaną operację przetwarzania[9]. Działanie takie musi mieć bowiem inną, „aktywną" formę. Przykładem może być naciśnięcie przycisku „przejście do serwisu"[10].

W kontekście powyżej określonego znaczenia zgody należy jeszcze ocenić skuteczność – na gruncie rozporządzenia 2016/679 – pozyskiwania zgody w sposób określony w art. 173 ust. 2 PT. Zgodnie z tym przepisem, „Abonent lub użytkownik końcowy może wyrazić zgodę, o której mowa w ust. 1 pkt 2, za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi". Podnoszony w praktyce problem dotyczy oceny, czy taki zapis nie stoi w sprzeczności z motywem 32 RODO, który pasywne działanie zakazuje traktować jako wyrażenie zgody. Chodzi tu w szczególności o sytuację, gdy domyślne ustawienie przeglądarki pozwala na automatyczną akceptację ciasteczek. Wydaje się jednak, że sytuacja taka „sama przez się" nie przekreśla możliwości zebrania ważnej zgody w ten sposób, o ile tylko zostaną spełnione wyżej określone warunki, tzn. instalacja *cookies* nie następuje przed wyrażeniem zgody (o której użytkownik został poinformowany), a akceptacja użytkownika ma formę wyraźnego działania potwierdzającego (np. kliknięcia określonego przycisku na stronie internetowej). Okoliczność, że użytkownik nie dokonał równocześnie zmian ustawień przeglądarki, jest wówczas bez znaczenia, w powyższym kontekście niedokonanie tej zmiany nie jest bowiem traktowane jako wyrażenie zgody, o jej skutecznym udzieleniu przesądzają bowiem inne elementy.

[9] Wytyczne Grupy Roboczej w sprawie zgody, s. 18.

[10] W Wytycznych dotyczących zgody podano jeszcze inne przykłady aktywnej zgody w środowisku „cyfrowym" – m.in. „Przesunięcie paska na ekranie, machnięcie przed inteligentną kamerą, obrócenie smartfona zgodnie z ruchem wskazówek zegara lub zakreślenie ósemki", Wytyczne Grupy Roboczej w sprawie zgody, s. 19.

Xawery Konarski
adwokat,
Traple Konarski Podrecki i Wspólnicy

RODO – 10 NAJWAŻNIEJSZYCH SKUTKÓW PRAWNYCH DLA BRANŻY REKLAMY INTERNETOWEJ

Przepisy RODO istotnie zmieniły sposób funkcjonowania firm internetowych i realizowanych przez nie procesów biznesowych. Dotyczy to również wykorzystywanych przez nie platform technologicznych oraz architektury danych, poprzez które zbierane, przechowywane i zarządzane są dane osobowe.

Poniżej przedstawiona została lista 10 najważniejszych skutków obowiązywania RODO z punktu widzenia branży reklamy internetowej.

Po pierwsze, przedmiotowy zakres zastosowania przepisów RODO jest szerszy niż miało to miejsce w poprzednim stanie prawnym. Za dane osobowe uznane zostały bowiem wszystkie identyfikatory internetowe, takie jak adresy IP czy identyfikatory plików *cookie* (art. 4, motyw 30 RODO). To samo dotyczy innych identyfikatorów, takich jak np. znaczniki (tagi) RFID (*Radio Frequency Identification*). W konsekwencji przepisami RODO objęte zostało szereg podmiotów, w stosunku do których nie stosowało się wcześniej przepisów o ochronie danych osobowych. Przykładem są firmy działające na rynku reklamy *programmatic*. Uznanie za dane osobowe znaczników RFID oznacza z kolei stosowanie się Rozporządzenia do szeregu projektów Internetu Rzeczy (*Internet of Things*, w sktórcie IoT), w szczególności wówczas gdy w ich ramach dochodzi do przetwarzania danych osobowych zebranych w ten sposób.

Po drugie, terytorialny zakres obowiązywania RODO jest szerszy niż poprzednio. Rozporządzenie znajduje bowiem zastosowanie do szeregu podmiotów niemających swoich jednostek organizacyjnych w Unii Europejskiej (np. siedziby, oddziału czy przedstawicielstwa). Będzie tak w szczególności wówczas, gdy przetwarzanie dotyczyć będzie danych osobowych osób przebywających w Unii, a czynności przetwarzania wiązać się będą z oferowaniem towarów lub usług takim osobom lub monitorowaniem ich zachowania (art. 3 ust. 2 RODO). Takie rozwiązanie jest wynikiem przyjętej w RODO koncepcji „długiego ramienia" ochrony na podstawie przepisów Rozporządzenia, obejmującego w pewnych sytuacjach również przetwarzanie dokonywane poza terytorium Unii Europejskiej. W związku z tym RODO stosuje się do szeregu firm internetowych mających swoje jednostki organizacyjne i przetwarzających dane osobowe poza Unią Europejską (UE). Przykładem są sklepy internetowe, serwisy społecznościowe, czy wyszukiwarki internetowe administrowane przez podmioty spoza UE, ale przetwarzające dane „osób przebywających w Unii".

Po trzecie, w RODO wprowadzono nowe kategorie podmiotów przetwarzających dane osobowe. W szczególności chodzi o współadministratorów danych, a więc podmioty, które wspólnie z innymi ustalają cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO) oraz „inne podmioty przetwarzające" (art. 28 ust. 2 i 4 RODO), tj. podwykonawców (procesorów) realizujących część powierzonych im operacji na danych osobowych. W zależności od rodzaju usługi oraz konkretnego sposobu jej świadczenia, obie te kategorie podmiotów przetwarzających dane osobowe mogą występować na rynku reklamy internetowej.

Po czwarte, istotnemu poszerzeniu uległ zakres informacji (art. 13-14 RODO), które powinny zostać przekazane podmiotowi danych (np. informacje o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu). Prawidłowe spełnienie tego obowiązku stanowi, z uwagi na różne formy reklamy internetowej, wyzwanie dla administratorów danych. Powszechnie stosowanym rozwiązaniem stało się „warstwowe" podawanie informacji (*layer approach*), tzn. przekazywanie bezpośrednio podmiotowi danych jedynie podstawowych informacji

(np. w formularzu rejestracyjnym na stronie internetowej), natomiast pozostałych informacji w kolejnych „warstwach" (np. dostępnych po naciśnięciu linku prowadzącego do rozbudowanej klauzuli informacyjnej). Tego rodzaju praktyka została usankcjonowana przez Grupę Roboczą Art. 29.

Po piąte, częściowo inaczej – niż dotychczas – określono przesłanki legalności przetwarzania danych osobowych. Z punktu widzenia reklamy internetowej znaczenie ma w szczególności nowe ujęcie konstrukcji prawnej zgody i warunków jej wyrażania przez podmioty danych (art. 4 pkt 11, art. 6 ust. 1 pkt a, art. 7-8 RODO), a także prawnie uzasadnionego interesu administratora danych (art. 6 ust. 1 pkt f). Istotnym *novum* jest w szczególności możliwość wyrażenia zgody nie tylko poprzez oświadczenie woli, ale również działanie konkludentne (np. zaznaczenie okna wyboru podczas przeglądania strony internetowej). Istotną zmianą jest również wprowadzenie możliwości, w przypadku danych wrażliwych (np. danych o stanie zdrowia), udzielenia zgody w sposób „wyraźny" (art. 9 ust. 2 a RODO), a nie – jak to było do tej pory – w formie pisemnej. Pozwala to na skuteczne zbieranie tego rodzaju zgód również w środowisku cyfrowym. Z uwagi na szczególną ochronę małoletnich w przepisach RODO wprowadzono także zasadę, że jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem (art. 8 RODO). W przypadku prawnie uzasadnionego interesu (*opt-out*) zwraca uwagę możliwość powołania się na tę przesłankę – w pewnych sytuacjach – również przy przetwarzaniu danych osobowych na „cudzy" cel marketingowy (art. 21 ust. 2 i 3, motywy 47-48 RODO). Administrator powinien przy tym wykonać tzw. test równowagi, a więc przeprowadzić ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu.

Po szóste, w RODO wprowadzono szczególną regulację dotycząca jednej z operacji na danych, tj. profilowania rozumianego jako „dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się" (art. 4 pkt 4 RODO). Z punktu widzenia branży reklamy internetowej kluczowe jest rozróżnienie „profilowania" zwykłego, wykonywanego na potrzeby marketingu bezpośredniego (art. 21 ust. 2-3 RODO) oraz profilowania „kwalifikowanego", wykonywanego na potrzeby „zautomatyzowanych decyzji", a więc decyzji podejmowanych bez udziału człowieka i mających istotne skutki prawne dla podmiotów danych (art. 22 RODO). Dla takiego profilowania w Rozporządzeniu wprowadzono dodatkowe gwarancje zabezpieczenia interesów podmiotów danych poprzez możliwość zakwestionowania automatycznie wydanej decyzji i jej ponownego zweryfikowania przy udziale człowieka (art. 22 ust. 3 RODO). W przypadku przetwarzania danych osobowych na potrzeby reklamy internetowej mamy jednak przeważnie do czynienia z profilowaniem „zwykłym", jego wykonywanie (np. poprzez automatyczne zestawienie danych o preferencjach zakupowych danej osoby) jest dopuszczalne do czasu wyrażenia przez tę osobę sprzeciwu (art. 21 ust. 3 RODO).

Po siódme, w RODO istotnie zmodyfikowano dotychczasowe lub ustanowiono zupełnie nowe prawa podmiotów danych. Chodzi tu w szczególności o: prawo dostępu do danych, w tym ich kopii (art. 15 RODO), prawo do bycia zapomnianym (art. 17 RODO), prawo do ograniczonego przetwarzania (art. 18 RODO) oraz prawo do przenoszalności danych (art. 20 RODO). Zapewnienie realizacji tych praw ma istotny wpływ na rodzaj wykorzystywanych narzędzi IT, a także ustanowienie wewnętrznych procedur przez firmy internetowe. Przykładowo, w przypadku prawa dostępu do danych organizacje muszą w pierwszej kolejności zidentyfikować dane dotyczące konkretnej osoby fizycznej ze wszystkich dostępnych źródeł, takich jakich systemy CRM, HR czy systemy archiwalne. Konieczna jest w związku z tym implementacja holistycznych narzędzi wyszukiwawczych pozwalających na odnalezienie tych danych. Od strony organizacyjnej istotne jest również stworzenie odpowiedniej procedury realizacji żądań podmiotów danych, zgodnej z art. 12 i n. RODO.

Po ósme, z uwagi na przyjęcie w RODO podejścia opartego na zasadzie ryzyka (*Risk Based Approach*), istotnej zmianie uległy wymogi dotyczące środków bezpieczeństwa danych, które muszą stosować podmioty przetwarzające dane osobowe. W pierwszej kolejności wymienić należy wymóg uwzględnienia ochrony danych osobowych w fazie projektowania (*privacy by design*, art. 25 ust. 1 RODO). Z jego realizacją związana może być między innymi analiza statyczna kodu programowania pod kątem ochrony danych. Podobny charakter ma zasada *privacy by default*, zgodnie z którą „Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania." (art. 25 ust. 2 RODO). W Rozporządzeniu wprowadzono także obowiązek zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku związanemu z zakresem i celem przetwarzania danych, z czym może się wiązać konieczność stosowania np. pseudonimizacji i szyfrowania danych osobowych (art. 32 ust. 1 pkt a RODO). W RODO nałożono również obowiązek dokonania, przed rozpoczęciem przewarzania danych osobowych, oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 RODO). Jeżeli ta ocena skutków wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania ma on obowiązek konsultacji z organem nadzorczym, tj. PUODO (art. 36 RODO).

Po dziewiąte, w RODO ustanowiono nowe instrumenty wykazywania zgodności z przepisami o ochronie danych osobowych (*compliance*). Zaliczyć do nich należy kodeksy postępowania oraz mechanizmy certyfikacji (art. 40 i n. RODO). Ich stosowanie istotnie może limitować ryzyka prawne związane z naruszeniem przepisów Rozporządzenia. Dla branży reklamy internetowej szczególne znaczenie może mieć w związku z tym Kodeks postepowania i dobrych praktyk branży reklamy internetowej, którego projekt przygotował Zespół RODO IAB Polska. Dla jego skuteczności jako mechanizmu *compliance* przewidzianego w RODO konieczne jest jeszcze jego zatwierdzenie przez organ nadzorczy (PUODO).

Po dziesiąte, w RODO przewidziano nowe sankcje administracyjne, w tym wysokie kary pieniężne za naruszenie przepisów o ochronie danych osobowych (art 83 RODO). Niezależnie od tego podmiot przetwarzający może ponosić również odpowiedzialność cywilną, w postaci odszkodowania lub zadośćuczynienia (art. 82 RODO). Z kolei w ustawie o ochronie danych osobowych wprowadzono odpowiedzialność karną za niedopuszczalne przetwarzanie danych osobowych albo przetwarzanie dokonywane przez nieupoważniony podmiot (art. 107 uodo).

STATUS PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE W RAMACH REKLAMY *PROGRAMMATIC*

Przemysław Szymański
LL. M.,
Head of Legal & Compliance,
RTB House SA

Uwagi wprowadzające

Przepisy RODO utrzymały tradycyjny podział podmiotów uczestniczących w procesach przetwarzania danych osobowych na „administratorów danych", tj. podmioty, które **samodzielnie lub wspólnie z innymi ustalają cele i sposoby przetwarzania danych osobowych,** oraz „podmioty przetwarzające", które przetwarzają dane osobowe **w imieniu administratorów (art. 4 pkt 7-8 RODO).**

Dodatkowo wprowadzono przepisy dotyczące współadministratorów danych (art. 26 RODO), odnoszące się do zawieranych pomiędzy nimi porozumień (art. 26 RODO). Równocześnie nie rozwiązano jednak w sposób kompleksowy praktycznych problemów interpretacyjnych, które pojawiły się w praktyce obrotu na gruncie stosowania Dyrektywy 95/46/WE i wzorowanej na niej polskiej ustawie o ochronie danych osobowych.

O ile przypisanie ról „administratora" lub „podmiotu przetwarzającego" podmiotom funkcjonującym w ramach tradycyjnych, „linearnych" relacji gospodarczych, w większości sytuacji nie stwarzało istotnych trudności, o tyle w przypadku nowych rynków, opartych na relacjach wielostronnych oraz szerokim wykorzystaniu danych w ramach powiązanych ze sobą operacji przetwarzania, kategoryczny podział ustawowo zdefiniowanych ról pomiędzy podmiotami aktywnymi na tych rynkach, wyłącznie w oparciu o ogólną przesłankę „decydowania o celach i sposobach przetwarzania", nie zawsze jest możliwy.

Problem ten jest szczególnie widoczny w przypadku reklamy internetowej (w szczególności reklamy *programmatic*/RTB*)* przede wszystkim z uwagi na stopień skomplikowania tego rynku i wykorzystywanych na nim technologii oraz różnorodność modeli funkcjonowania podmiotów aktywnych w jego poszczególnych segmentach. W konsekwencji brak jest jednolitego stanowiska uczestników rynku w zakresie określania ról w poszczególnych procesach przetwarzania danych tworzących ekosystem reklamy internetowej.

Mając na uwadze powyższe, w niniejszym rozdziale zostały przedstawione kryteria pomocnicze, specyficzne dla branży reklamy internetowej, które mogą być stosowane przez podmioty z tej branży do określania swoich ról w ramach konkretnych procesów przetwarzania danych wraz z propozycjami kwalifikacji relacji pomiędzy poszczególnymi uczestnikami rynku reklamy *programmatic*.

Rynek programmatic/RTB

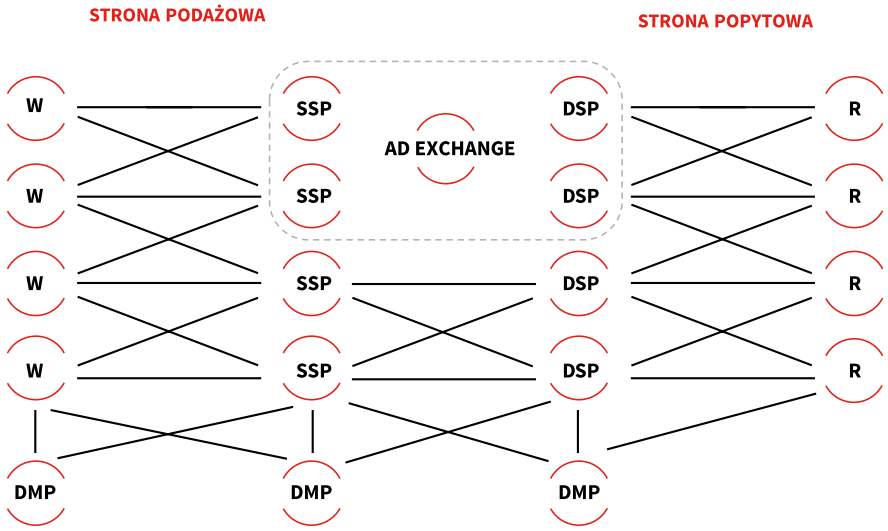
Struktura i uczestnicy rynku

Rynek reklamy *programmatic* funkcjonuje w oparciu o model nabywania powierzchni reklamowej dostępnej na stronach internetowych lub w aplikacjach mobilnych w sposób zautomatyzowany, przy użyciu dedykowanego oprogramowania i algorytmów. Istotnym i stale rosnącym segmentem rynku *programmatic* jest rynek RTB (*Real-Time Bidding*), w ramach którego proces nabywania powierzchni reklamowej odbywa się w trybie aukcji prowadzonych w czasie rzeczywistym. Pozostałą część rynku stanowi segment *programmatic direct*, na którym reklamodawcy (agencje) nabywają powierzchnię reklamową bezpośrednio od wydawców na indywidualnie określonych warunkach.

Rynek *programmatic* funkcjonuje w oparciu o identyfikatory internetowe (*cookie ID, mobile advertising ID*) oraz powiązane z nimi dane behawioralne, które łącznie na gruncie RODO traktowane są jako dane osobowe. Aukcje w systemie RTB prowadzone są na podstawie ogólnie przyjętych protokołów (w szczególności protokołu OpenRTB), które określają ich szczegółowy przebieg oraz kategorie danych, które mogą być przesyłane w ramach aukcji. Głównymi uczestnikami rynku *programmatic* są:

- wydawcy, tj. operatorzy stron internetowych, udostępniający na nich powierzchnię reklamową (tzw. *inventory*) o określonych parametrach;
- platformy SSP (*Supply Side Platforms*), tj. platformy podażowe, oferujące powierzchnie reklamowe dostępne na stronach wydawców platformom DSP, bezpośrednio lub poprzez tzw. giełdy reklam (*Ad Exchange*);
- platformy DSP (*Demand Side Platforms*), tj. platformy popytowe, umożliwiające reklamodawcom zarządzanie procesem zakupu powierzchni reklamowej dostępnej na stronach wydawców;
- platformy DMP (*Data Management Platforms*), tj. platformy zarządzania danymi, dostarczające dane o użytkownikach (lub segmenty tych danych, opracowane w oparciu o kryteria behawioralne lub demograficzne) i umożliwiające wykorzystywanie przez reklamodawców danych z różnych źródeł w celu optymalizacji kampanii reklamowych;
- reklamodawcy (lub agencje interaktywne i domy mediowe działające w imieniu reklamodawców), zlecający platformom DSP (w modelu *Real-Time Bidding*) lub wydawcom (w modelu *programmatic direct*) realizację kampanii reklamowych ich produktów i usług.

STRUKTURA RYNKU RTB



W – wydawca, **R** – reklamodawca.

6. Schemat struktury rynku RTB

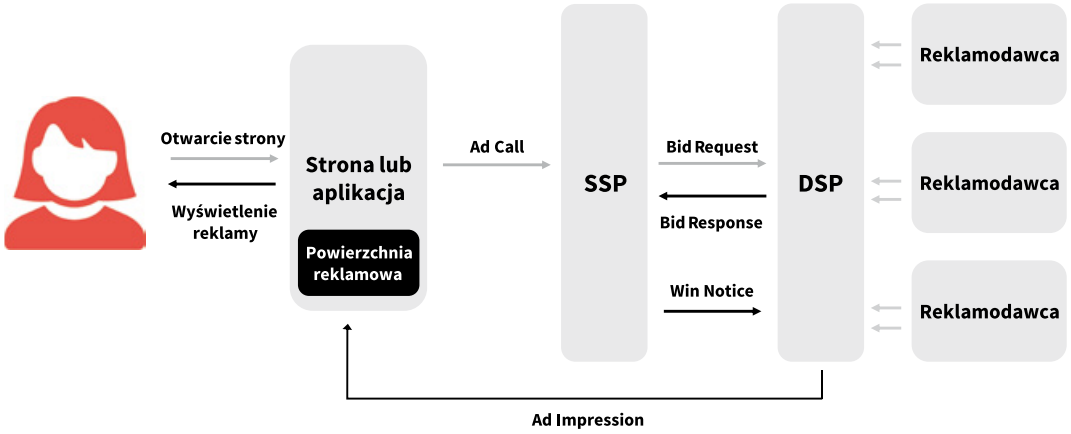
Przebieg aukcji w systemie RTB

Aukcje powierzchni reklamowej w modelu RTB oraz związane z nim transfery danych odbywają się w kilku etapach, których łączny czas trwania wynosi ok. 300 milisekund:

- aukcja zostaje zainicjowana w momencie wejścia użytkownika na stronę internetową wydawcy; wówczas skrypty platformy SSP zainstalowane na stronie inicjują instalację identyfikatora internetowego na urządzeniu końcowym użytkownika lub odczytanie identyfikatora już zainstalowanego na urządzeniu (tj. *cookie ID* lub *mobile advertising ID*) oraz powodują wysłanie komunikatu o dostępnej powierzchni reklamowej (*Ad Call*) do platformy SSP;
- po otrzymaniu komunikatu *Ad Call* platforma SSP przesyła do zintegrowanych z nią platform DSP lub giełd reklam zaproszenie do składania ofert na określoną powierzchnię reklamową ze wskazaniem

m.in. jej formatu i adresu domeny (tzw. *Bid Request*) wraz z informacjami o użytkowniku, któremu reklama może zostać wyświetlona (m.in. *cookie ID*, informacje o urządzeniu końcowym użytkownika);
- platformy DSP dokonują wyceny wyświetlenia reklamy na podlegającej aukcji powierzchni reklamowej (np. w oparciu o parametry wyświetlenia – rozmiar banera reklamowego, jego położenie na stronie – czy dane o użytkowniku uzyskane od reklamodawców, na rzecz których działają lub dane segmentowe od platform DMP) i wysyłają swoje oferty (*Bid Response*);
- platforma DSP, która zaoferowała najwyższą cenę za wyświetlenie reklamy, otrzymuje odpowiednią notyfikację o wygranej aukcji (*Win Notice*) i wysyła dedykowaną grafikę lub wideo (*Ad Impression*) na powierzchnię reklamową.

PRZEBIEG AUKCJI W SYSTEMIE RTB



7. Schemat przebiegu aukcji w systemie RTB

Kryteria określania statusu podmiotu w procesach przetwarzania danych

W ramach aukcji RTB funkcjonują w obiegu dwie kategorie danych osobowych, powiązanych z unikalnymi identyfikatorami internetowymi, tj.:
- dane zawarte w ofertach wyświetlenia reklam na stronach wydawców (*Bid Requests*), rozsyłanych przez platformy SSP; kategorie obowiązkowych, rekomendowanych i opcjonalnych danych, które powinien (może) zawierać *Bid Request* określone są protokołem OpenRTB i obejmują m.in. adres IP (pełny lub okrojony), informacje o urządzeniu użytkownika, adres URL dostępnej powierzchni reklamowej (pełny lub okrojony), kategorię treści dostępnej na stronie (np. sport, muzyka itp.);
- dane segmentowe (behawioralne, demograficzne) uzyskane ze stron internetowych i systemów CRM reklamodawców lub udostępniane przez platformy DMP, wykorzystywane do optymalizacji wyceny powierzchni reklamowych w ramach aukcji RTB.

Określony podmiot w ramach powiązanych procesów przetwarzania danych może być administratorem w odniesieniu do jednego zestawu danych i podmiotem przetwarzającym w stosunku do innego, przy czym w niektórych okolicznościach zakresy tych oddzielnych zbiorów danych w pewnym stopniu mogą się pokrywać (np. dane powiązane z jednym identyfikatorem internetowym mogą być wykorzystywane w odrębnych procesach przetwarzania, prowadzonych na rzecz różnych podmiotów).

Biorąc pod uwagę wskazane wcześniej problemy przy ustalaniu statusu poszczególnych uczestników rynku RTB w odniesieniu do przetwarzanych zbiorów danych, rekomendowane jest uwzględnienie

przez podmioty z branży kryteriów pomocniczych wskazanych poniżej[11], przy czym należy zauważyć, że spełnienie przez dany podmiot jednego lub więcej z tych kryteriów może, lecz nie musi, spowodować uznania takiego podmiotu za administratora danych. Zgodnie bowiem z opinią Grupy Roboczej Art. 29 „pojęcie administratora danych jest pojęciem funkcjonalnym, mającym na celu przypisanie obowiązków tam, gdzie występuje faktyczny wpływ, a zatem raczej w oparciu o analizę okoliczności faktycznych niż o analizę formalną".[12]

a) Tworzenie unikalnego identyfikatora użytkownika (UID)

Jeśli w ramach określonej operacji przetwarzania danych podmiot tworzy unikalny identyfikator użytkownika (np. przy instalacji pliku *cookie* w przeglądarce użytkownika) wyłącznie lub częściowo dla własnych celów, należy uznać, że w typowej sytuacji podmiot taki pełnić będzie rolę administratora w stosunku do danych przypisanych do tego identyfikatora.

Jeżeli natomiast w ramach danej operacji przetwarzania podmiot tworzy lub używa identyfikatora wyłącznie dla celów świadczenia usług na rzecz swojego klienta (klientów), podmiot ten w tym zakresie powinien być uznany za podmiot przetwarzający dane, ponieważ działa „w ramach" celu określonego już klienta zlecającego realizację danej usługi (przy czym używanie tego samego identyfikatora dla różnych klientów może w określonych sytuacjach powodować uznanie podmiotu za administratora danych – zgodnie z pkt b) poniżej).

Podmioty wykorzystujące identyfikatory (takie jak np. *mobile advertising ID*) utworzone przez podmioty trzecie, takie jak dostawcy systemów operacyjnych (iOS, Android), w celu określenia swojego statusu powinny korzystać z pozostałych kryteriów pomocniczych.

b) Sposób korzystania z identyfikatora użytkownika i powiązanych z nim danych

Jeżeli podmiot wykorzystuje ten sam identyfikator użytkownika w ramach świadczenia usług na rzecz kilku klientów i nie jest umownie ani technicznie ograniczony w wykorzystywaniu tego identyfikatora na cele inne niż wykonywanie instrukcji poszczególnych klientów, można przyjąć, że w typowej sytuacji podmiot taki powinien zostać uznany za administratora danych przypisanych do tego identyfikatora. W sytuacjach tych podmiot, w ramach korzystania ze wspólnego identyfikatora użytkownika, ma bowiem faktyczną możliwość wykorzystania powiązanych z nim danych przetwarzanych w związku ze świadczeniem usług na rzecz różnych klientów, np. w celu optymalizacji częstotliwości wyświetlania reklam dla danego użytkownika (*frequency capping*) lub budowania bardziej kompleksowych profili behawioralnych, co należy uznać za jednoznaczne z określaniem celów i zasadniczych sposobów przetwarzania danych.

W przypadku natomiast gdy określony podmiot używa osobnego identyfikatora w stosunku do każdego klienta lub mimo wykorzystania wspólnego identyfikatora użytkownika, dokonuje logicznej separacji danych zebranych w ramach świadczenia usług na rzecz poszczególnych klientów i poszczególne podzbiory danych wykorzystuje wyłącznie na cele świadczenia usług na rzecz odpowiednich klientów i zgodnie z ich instrukcjami, wówczas podmiot ten powinien zostać uznany za podmiot przetwarzający dane w odniesieniu do takich odrębnych procesów przetwarzania.

Należy również zwrócić uwagę, że dany **unikalny identyfikator użytkownika może być powiązany z oddzielnymi zestawami danych przetwarzanymi przez jeden podmiot**, w odniesieniu do których ten podmiot można uznać zarówno za administratora, jak i za podmiot przetwarzający ten identyfikator w ramach odrębnych procesów przetwarzania (np. odrębne zbiory danych przypisane do

[11] Przy opracowywaniu kryteriów wskazanych w niniejszym raporcie uwzględniono publikację IAB Europe GDPR Implementation Group Working Paper 05/2018 „Controller-Processor Criteria", Version 1.0, 19/07/2018, dostępną na stronie: https://www.iabeurope.eu/wp-content/uploads/2018/07/20180719-IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

[12] Opinia Grupy Roboczej Art. 29 nr 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", przyjęta dnia 16 lutego 2010 r., WP 169, s. 11.

określonego *cookie ID* mogą być przetwarzane przez platformę DSP lub platformę DMP na rzecz różnych klientów, jak również w celach własnych).

c) Określenie zakresu i kategorii przetwarzanych danych

Jeżeli w związku ze świadczeniem usług na rzecz swojego klienta dany podmiot posiada pełną autonomię przy określaniu zakresu danych, które będą zbierane za pomocą technologii opartej na unikalnych identyfikatorach, decyduje o odbiorcach tych danych oraz ustala, przez jaki okres dane te będą przetwarzane, taki podmiot w typowej sytuacji może zostać uznany za administratora (współadministratora) danych z uwagi na to, że określa zasadnicze sposoby przetwarzania danych.

Jeżeli natomiast zakres danych zbieranych i przetwarzanych przez podmiot jest determinowany lub ostatecznie zatwierdzany przez jego klienta (np. poprzez zaakceptowanie standardowego wzorca umowy, jednak przy zachowaniu możliwości modyfikacji zakresu przetwarzania danych), w typowej sytuacji podmiot taki powinien zostać uznany za podmiot przetwarzający, należy bowiem przyjąć, że określa on jedynie techniczne aspekty przetwarzania danych.

Typowe role uczestników rynku RTB w procesach przetwarzania danych

Jak zostało wskazane powyżej, wprowadzenie jednolitej typologii relacji między podmiotami działającymi na rynku *programmatic*/RTB w zakresie przetwarzania danych osobowych napotyka w praktyce trudności. Poniżej przedstawiona kwalifikacja relacji pomiędzy głównymi uczestnikami rynku *programmatic* w odniesieniu do ich ról w procesie przetwarzania danych powinna być więc traktowana jako próba systematyzacji, oparta na zaobserwowanej praktyce kontraktowej oraz uwzględniająca stanowiska wyrażone w opiniach Grupy Roboczej Art. 29 oraz dotychczasowym orzecznictwie Trybunału Sprawiedliwości UE („TSUE"). Należy jednak podkreślić, że ostateczne ustalenie roli określonego podmiotu w procesie przetwarzania w konkretnej sytuacji będzie możliwe dopiero na podstawie szczegółowej analizy faktycznych okoliczności, w szczególności technicznych aspektów tego procesu przetwarzania.

Wydaje się, że co do zasady duża część podmiotów na rynku RTB powinna, przynajmniej w odniesieniu do części podejmowanych operacji przetwarzania danych osobowych, przyjąć rolę administratora danych, przede wszystkim z uwagi na fakt, że wiele z nich nadaje użytkownikom unikalne identyfikatory internetowe i w istotnej części ma wpływ na zakres przetwarzanych danych. Pozostają jednak grupy operacji przetwarzania danych, w których z uwagi na relacje kontraktowe i okoliczności faktyczne będziemy mieć do czynienia z relacją administrator – podmiot przetwarzający.

Należy również zaznaczyć, że w przypadku gdy w ramach jednej kampanii reklamowej dane są przetwarzane w tym samym celu (np. marketingowym) przez więcej niż jeden podmiot, nie czyni ich to jednak automatycznie współadministratorami danych. Kwestię (współ)administrowania danymi należy bowiem zawsze oceniać w odniesieniu do indywidualnej operacji przetwarzania danych, a nie w odniesieniu do nieokreślonego zbioru wszystkich czynności określanych mianem przetwarzania w ramach określonego rynku.[13]

Mając na uwadze powyższe, wydaje się, że na gruncie reklamy *programmatic* tak rozumiana koncepcja współadministrowania danymi osobowymi nie będzie mieć szerokiego zastosowania. Jednocześnie należy zauważyć, że tendencja do automatycznego stosowania tej konstrukcji do procesów, w których uczestniczy dwóch lub więcej administratorów danych, niekoniecznie będzie gwarantować wyższy poziom ochrony podstawowych praw i wolności podmiotów danych, co bywa wskazywane jako przesłanka do rozszerzającej interpretacji pojęcia współadministrowania.[14]

a) Wydawca – platforma SSP

W ramach systemu RTB wydawca udostępnia platformom SSP i innym podmiotom przestrzeń reklamową na swojej stronie internetowej. Umożliwia im również instalowanie plików *cookie* na urządzeniach końcowych użytkowników internetu odwiedzających strony wydawcy i stosowanie innych technologii umożliwiających przetwarzanie danych tych użytkowników w celu wyświetlania spersonalizowanej reklamy.

W odniesieniu do roli wydawcy w procesie przetwarzania danych osobowych użytkowników należy odwołać się do stanowiska wyrażonego w Opinii 1/2010 Grupy Roboczej Art. 29, zgodnie z którym co do zasady „wydawcę należy uznać za niezależnego administratora danych, w zakresie w jakim gromadzi on dane osobowe od użytkowników (profil użytkownika, adres IP, lokalizacja, język systemu operacyjnego itp.) dla własnych celów". Dodatkowo, „w zależności od warunków współpracy pomiędzy wydawcą a dostawcą sieciowej reklamy, jeśli na przykład wydawca umożliwia przekazywanie danych osobowych dostawcy sieciowej reklamy, w tym poprzez przekierowanie użytkownika na stronę internetową dostawcy reklamy sieciowej, mogą oni być wspólnymi administratorami (*joint controllers*) dla grupy operacji przetwarzania danych prowadzących do marketingu behawioralnego".[15]

Do określenia platform SSP w procesie przetwarzania zastosowanie mogą mieć natomiast fragmenty przywołanej wyżej opinii w zakresie dotyczącym „dostawcy reklamy sieciowej" (*ad network provider*), kwalifikujące ten podmiot jako administratora danych, z uwagi na fakt, iż „określa on cele (monitorowanie użytkowników na stronach internetowych) lub podstawowe sposoby przetwarzania danych".[16] Zgodnie z Opinią 2/2010 Grupy Roboczej Art. 29 „operatorzy sieci reklamowych mają całkowitą kontrolę nad celami i środkami przetwarzania. „Wynajmują" przestrzeń na stronach internetowych wydawców, aby umieszczać w niej reklamy; określają i odczytują informacje dotyczące plików cookie oraz, w większości przypadków, gromadzą adresy IP i inne ewentualne dane, jakie można uzyskać z przeglądarki. (…)".[17] Stanowisko to wynika z faktu, iż w ramach współpracy wydawcy nie udzielają platformom SSP żadnych instrukcji w zakresie procesów przetwarzania danych. Platformy SSP działają w sposób niezależny od wydawców, określając zakres danych, jakie zostają zbierane na stronie wydawcy za pomocą własnych kodów, krąg odbiorców tych danych (platformy DSP, DMP), okres retencji danych, jak również zakres danych wysyłanych do poszczególnych odbiorców.

[13] Tak opinia Rzecznika Generalnego Michała Bobka przedstawiona w dniu 19 grudnia 2018 r. w sprawie C-40/17, Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW e.V.

[14] Tak wyrok z dnia 5 czerwca 2018 r., Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, pkt 42.

[15] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", s. 25.

[16] Ibid., s. 25-26.

[17] Opinia 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta dnia 22 czerwca 2010 r., WP 171, s. 12.

b) Platforma SSP – platforma DSP

Fragmenty przytoczonej powyżej opinii Grupy Roboczej Art. 29 nr 1/2010 znajdują także zastosowanie w odniesieniu do relacji pomiędzy platformą SSP i platformą DSP z uwagi na fakt, że oba te podmioty można uznać za realizujące w odpowiednich częściach zadania zarezerwowane wcześniej dla wspomnianych w opinii „dostawców reklamy sieciowej". Należy więc przyjąć, że zarówno platformy SSP, jak i DSP są niezależnymi administratorami danych zawartych w ofertach wyświetlenia reklam (*Bid Requests*), takich jak dane o wizycie użytkownika na stronie internetowej, przypisanych do jego identyfikatora internetowego.

Platforma DSP we własnym zakresie podejmuje decyzje, czy odpowiedzieć na daną ofertę wyświetlenia reklamy, jaką cenę wyświetlenia wskazać w aukcji RTB i reklamę którego ze swoich klientów wyświetlić oraz czy wykorzystywać dane otrzymane od platformy SSP w innym celu niż udział w danej aukcji (np. wzbogacanie profili zidentyfikowanych użytkowników, tzw. *frequency capping*, opracowywanie statystyk wyświetleń reklam na cele optymalizacji kampanii), a więc określa cele przetwarzania. Podejmuje również decyzje w zakresie zasadniczych sposobów przetwarzania danych otrzymywanych od platformy SSP poprzez określanie zakresu przetwarzania danych zawartych w ofertach wyświetlenia reklamy (tj. określenie, które dane zawarte w ofercie wyświetlenia reklamy przetwarzać na cele udziału w aukcji) oraz okres ich przechowywania po zakończeniu aukcji. Z obserwacji dotychczasowej praktyki obrotu wynika, że w zdecydowanej większości przypadków platformy SSP i platformy DSP określają swoje relacje jako współpracę niezależnych administratorów. Nawet jeżeli platforma SSP w ramach umowy z platformą DSP określa niektóre parametry przetwarzania danych (np. zakaz tworzenia profili w celu ich odsprzedaży, zakaz łączenia z danymi bezpośrednio identyfikującymi), takie ustalenia stron należy postrzegać jako wyraz ich swobody kontraktowej, nie zaś jako instrukcje udzielane przez platformę SSP platformie DSP, charakterystycznej dla relacji administrator – podmiot przetwarzający.

c) Reklamodawca – platforma DSP

W sytuacji gdy reklamodawca umożliwia platformie DSP zbieranie na jego stronie internetowej danych o aktywności użytkowników odwiedzających tę stronę, np. w celu późniejszego wyświetlania im na stronach wydawców reklam kategorii produktów, które wcześniej oglądały (tzw. *retargeting*), wówczas platformę DSP można uznać za podmiot przetwarzający dane na rzecz reklamodawcy działającego jako administrator danych. To bowiem reklamodawca inicjuje proces przetwarzania poprzez zlecenie prowadzenia kampanii reklamowej (określa cele przetwarzania), jak również na podstawie umowy z platformą DSP ma kontrolę nad zasadniczymi aspektami przetwarzania danych m.in. poprzez decydowanie, na których spośród jego stron internetowych ma następować zbieranie danych, określanie rodzajów kodów, które zostaną użyte w ramach zbierania danych oraz udostępnianie dodatkowych danych o użytkownikach, np. w celu wyświetlania im reklam na różnych urządzeniach (tzw. *cross-device tracking*).

Należy jednak podkreślić, że platforma DSP może być uznana za podmiot przetwarzający tylko w zakresie, w jakim wykorzystuje te dane do realizacji celów określonych przez reklamodawcę (tj. budowania profili marketingowych użytkowników w celu prezentowania im reklam produktów i usług tego reklamodawcy). W sytuacji gdy wykorzystuje wskazane dane w celu prowadzenia kampanii reklamowych innych klientów (w szczególności poprzez tworzenie jednego profilu behawioralnego użytkownika na potrzeby wielu kampanii prowadzonych na rzecz różnych klientów), przyjmuje wówczas rolę niezależnego administratora danych i wynikające z tego statusu obowiązki.

W sytuacji gdy reklamodawca w ramach współpracy z platformą DSP nie przekazuje jej danych (np. ze swojego systemu CRM) ani nie umożliwia jej zbierania danych ze swojej strony internetowej, a jedynie określa ogólne kryteria, którymi powinna się kierować platforma DSP przy wyborze adresatów określonej kampanii reklamowej, wówczas trudno go uznać za administratora danych przetwarzanych przez platformę DSP w ramach realizowanych na jego rzecz kampanii. Taki reklamodawca nie tylko bowiem nie ma dostępu do danych osobowych przetwarzanych w ramach aukcji RTB (co

samo w sobie nie stoi na przeszkodzie uznaniu go za administratora danych[18]), ale przede wszystkim nie ma żadnego wpływu na wynik poszczególnych aukcji ani na sposób wykorzystania danych z tych aukcji przez platformę DSP, a więc nie określa celów ani sposobów poszczególnych procesów przetwarzania danych w ramach aukcji. Posiada jedynie ogólny interes gospodarczy w realizacji kampanii reklamowej, co nie jest wystarczającą przesłanką uznania za administratora danych.

d) Wydawca – platforma DMP

W ramach relacji z platformami DMP wydawcy poprzez odpowiednie ustawienia swojej strony internetowej umożliwiają instalację w urządzeniu końcowym użytkowników plików *cookie* dla potrzeb monitorowania ich aktywności na stronie i tworzenia na podstawie zebranych danych grup docelowych użytkowników (segmentacja). Należy uznać, że tak jak w przypadku relacji wydawca – platforma SSP (por. pkt a) powyżej), zarówno wydawca, jak i platforma DMP działają jako **niezależni administratorzy danych** z uwagi na fakt, iż wydawca umożliwia (inicjuje) zbieranie danych przez platformę DMP, która następnie w pełni autonomicznie decyduje o sposobach ich dalszego wykorzystania.

e) Reklamodawca – platforma DMP

W przypadku, gdy reklamodawca udostępnia platformie DMP dane osobowe użytkowników w celu ich integracji i wykorzystania na potrzeby realizacji kampanii reklamowych tego reklamodawcy, platforma DMP będzie przeważnie pełniła rolę podmiotu przetwarzającego dane na rzecz reklamodawcy (w zakresie, w jakim wykorzystuje te dane wyłącznie we wskazanym powyżej celu). Natomiast w sytuacji, gdy platforma DMP udostępnia reklamodawcy dane segmentowe użytkowników uzyskane wcześniej we własnym zakresie, relacja tych podmiotów powinna zostać uznana za relację niezależnych administratorów.

f) Platforma DMP – platforma DSP

W sytuacji gdy platforma DMP w ramach prowadzonej kampanii reklamowej udostępnia platformie DSP segmenty danych, platforma DSP pełni rolę podmiotu przetwarzającego, ponieważ nie decyduje o środkach i celach przetwarzania (sytuacja analogiczna do relacji reklamodawca – platforma DSP). Platforma DSP może również nabywać segmenty danych od platformy DMP w celu optymalizacji prowadzonych kampanii, co będzie skutkowało powstaniem relacji administrator – administrator (przy założeniu, że platforma DSP realizuje własne cele przetwarzania danych).

[18] Tak wyrok TSUE z dnia 10 lipca 2018 r., C-25/17, Jehovan todistajat.

STATUS PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE W „TRADYCYJNEJ" REKLAMIE INTERNETOWEJ ZE SZCZEGÓLNYM UWZGLĘDNIENIEM E-MAIL MARKETINGU

Jakub Borkowski
inspektor ochrony danych, Netsprint S.A., Leadr sp. z o. o.

Jan Tyski
radca prawny, inspektor ochrony danych, Tarsago Polska sp. z o. o.

Uwagi wstępne

„Tradycyjna" reklama internetowa polega na zleceniu kampanii reklamowej przez **Klienta (Reklamodawcę)**, realizowanej przez publikowanie treści reklamowych (tzw. kreacja) na powierzchni oferowanej przez **Wydawcę** (np. na stronie WWW lub w aplikacji mobilnej) lub prowadzonej w formie kampanii e-mail marketingowej, zawierającej reklamę Klienta. W przeciwieństwie do modelu reklamy typu *programmatic* udzielenie zlecenia nie odbywa się za pomocą platformy informatycznej, będącej w istocie giełdą ofert, lecz bezpośrednio poprzez działy handlowe poszczególnych podmiotów zaangażowanych w proces.

Mimo że zdarzają się przypadki bezpośredniej współpracy pomiędzy Reklamodawcą i Wydawcą, to jednak **w zdecydowanej większości przypadków w proces zaangażowani są liczni pośrednicy działający na rzecz Klienta lub Wydawcy**. Pośrednicy ci mogą współpracować zarówno bezpośrednio z Wydawcą/Klientem, jak również zlecać realizację innym Pośrednikom, skutkiem czego liczba ogniw w łańcuchu zleceń może się znacznie wydłużać. Potrzeba angażowania Pośredników wynika przede wszystkim z ich wyspecjalizowania na danym etapie procesu, czego wynikiem jest optymalne przeprowadzenie kampanii marketingowej.

Tradycyjna reklama internetowa – kategorie podmiotów

Nazewnictwo kategorii podmiotów uczestniczących w realizacji kampanii może przyjąć różne formy w zależności od przyjętego kryterium, np. sposobu rozliczeń (np. sieci afiliacyjne), obszaru emisji (np. sieci *mobile*) czy zakresu zadań (np. agencje kreatywne, agencje interaktywne, firmy analityczne).

W niniejszym raporcie autorzy proponują następującą klasyfikację:

- **Klient (Reklamodawca)** – podmiot, na rzecz którego realizowana jest kampania reklamowa.
- **Pośrednik Klienta (Pośrednik Reklamodawcy)** – pośrednik działający na rzecz Reklamodawcy, np. dom mediowy, który odpowiedzialny jest za dobór i zakup mediów.
- **Pośrednik Wydawcy (Pośrednik Dysponenta Bazy)** – pośrednik działający na rzecz Wydawców, np. sieci reklamowe, brokerzy oferujący powierzchnie Wydawców lub – w przypadku e-mail marketingu – Pośrednik Dysponenta bazy sprzedający zasoby bazodanowe Dysponenta bazy.
- **Wydawca (Dysponent Bazy**) – Administrator serwisu WWW lub aplikacji, gdzie oferowana jest powierzchnia reklamowa lub – w przypadku e-mail marketingu – Dysponent Bazy adresów e-mail wykorzystywanych do wysyłki e-mail marketingowej.

W celu ustalenia statusu „administratora" lub „podmiotu przetwarzającego" w myśl art. 4 pkt 7 - 8 RODO trzeba ocenić, kto ustala cele i sposoby przetwarzania danych osobowych. Należy przy tym dokonać analizy, np. kto ma wpływ na ustalenie konkretnego zestawu danych, a nie opierać się na roli (nazwie), jaką ma dany podmiot w łańcuchu reklamowym.

W świetle powyższego, ten sam podmiot może być bowiem administratorem w stosunku do jednego zestawu danych i procesorem w stosunku do innego zestawu danych. Przykładowo, często spotykaną praktyką jest, że w kreacji reklamowej poszczególne podmioty umieszczają tzw. kody śledzące, co pozwala im mierzyć efektywność realizacji kampanii m.in. poprzez liczbę wyświetleń reklamy,

liczbę kliknięć czy liczbę unikalnych użytkowników. Zwykle administratorami poszczególnych zestawów danych są podmioty, które je umieściły w kreacji reklamy, w pewnych jednak sytuacjach status taki mogą mieć również inne podmioty. Bez znaczenia jest przy tym, czy dysponują one dostępem do zestawu danych wykorzystywanego w reklamie.

W opinii autorów wykładni, zgodnie z którą Klient jest administratorem każdego zestawu danych przetwarzanego w procesie tradycyjnej reklamy internetowej nie można stosować automatycznie i kwestia ta wymaga każdorazowo dokonania odpowiedniej analizy. Jak bowiem wskazano w opinii Grupy Roboczej Art. 29 (obecnie: Europejska Rada Ochrony Danych) „pojęcie administratora danych jest pojęciem funkcjonalnym, mającym na celu przypisanie obowiązków tam, gdzie występuje faktyczny wpływ, a zatem raczej w oparciu o analizę okoliczności faktycznych niż o analizę formalną. Określenie kontroli może zatem wymagać niekiedy szczegółowej i długiej analizy”[19].

Administrator danych w reklamie internetowej – kryteria pomocnicze

W celu ustalenia statusu podmiotów z branży reklamy internetowej w odniesieniu do każdego zestawu danych zalecane jest użycie **kryteriów pomocniczych**[20] wymienionych poniżej. Należy jednak mieć na uwadze, że spełnienie tych kryteriów przesądza o uznaniu danego podmiotu za administratora w sytuacjach typowych. W konkretnym stanie faktycznym możliwe będzie dokonanie innej kwalifikacji.

Tworzenie unikalnego identyfikatora użytkownika (UID)

Czy dany podmiot tworzy unikalny identyfikator użytkownika (UID) wyłącznie lub nawet częściowo dla własnych celów?

Spełnienie powyższego warunku oznacza zwykle pełnienie roli administratora, w stosunku do danych przypisanych do wybranego identyfikatora. W przypadku jednak, gdy identyfikatora używa się wyłącznie do świadczenia usług innemu podmiotowi, to przeważnie przyjąć należy, że podmiot przetwarzający informacje przypisane do identyfikatora pełni rolę procesora.

Sposób korzystania z identyfikatora użytkownika i powiązanych z nim danych

Czy unikalny identyfikatory użytkownika jest współdzielony pomiędzy kampanie świadczone dla różnych klientów (identyfikator globalny)?

Użycie tego samego identyfikatora użytkownika w kampaniach realizowanych na rzecz różnych podmiotów może świadczyć o pełnieniu roli administratora z powodu **faktycznej możliwości użycia danych do realizacji własnych celów**.

W przypadku gdy ograniczona jest możliwość użycia identyfikatora do własnych celów, przykładowo poprzez:

- użycie różnych identyfikatorów dla tego samego użytkownika w różnych kampaniach (tj. w kampanii X użytkownik posiada identyfikator X1234, a w kampanii Y użytkownik posiada identyfikator Y1324),
- zapisy w umowie pomiędzy stronami wykluczające użycie identyfikatora do własnych celów,

kryterium nie jest spełnione i zwykle oznacza to pełnienie roli procesora przetwarzającego dane osobowe na rzecz innego podmiotu.

[19] Opinia Grupy Roboczej Art. 29 nr 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”, przyjęta dnia 16 lutego 2010 r., WP 169, s. 11.

[20] Przy opracowywaniu kryteriów pomocniczych uwzględniono publikację IAB Europe GDPR Implementation Group Working, Paper 05/2018 „Controller-Processor Criteria”, Version 1.0, 19/07/2018, dostępną na stronie: https://www.iabeurope.eu/wp-content/uploads/2018/07/20180719-IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

Określenie zakresu i kategorii przetwarzanych danych

Czy dany podmiot określa, jakie dane (kategorie danych) o użytkowniku mają być zbierane i przypisane do unikalnego identyfikatora?

Określenie, jakie dane są zbierane i przypisanie ich do identyfikatora użytkownika, może świadczyć o fakcie decydowania o celach i sposobach przetwarzania danych, a w konsekwencji o statusie administratora danych. W przypadku gdy zakres zbieranych danych narzucony jest przez inny podmiot, np. zleceniodawcę i zbierane dane nie wykraczają poza określony przez niego zakres, kryterium nie jest spełnione i zwykle oznacza pełnienie roli podmiotu przetwarzającego (procesora) na rzecz podmiotu, który określił zakres zbierania danych.

W świetle powyższego należy podkreślić zasadniczą różnicę pomiędzy emisją kampanii na powierzchniach reklamowych a realizacją kampanii e-mail marketingowych. W serwisie WWW użytkownik najpierw wyświetla stronę serwisu, a następnie występuje emisja reklamy. Natomiast w kampaniach e-mailingowych najpierw Wydawca (Dysponent Bazy) lub Pośrednik Wydawcy (Pośrednik Dysponenta Bazy) wysyła wiadomości e-mail, a dopiero następnie użytkownik może, aczkolwiek nie musi, wyświetlić treść reklamy. Powyższa kwestia, w opinii autorów, powoduje, że warto dokonać bardziej szczegółowej analizy roli podmiotów uczestniczących w kampanii w odniesieniu do adresów e-mail, które zostały użyte do wysyłki reklamowej.

E-mail marketing

W najprostszym wariancie realizacja e-mail marketingu (w założeniu, że Reklamodawca nie realizuje go w całości samodzielnie) opiera się na schemacie: **Klient** – **Pośrednik Klienta** (podmiot realizujący wysyłkę na bazie dostarczonej przez Reklamodawcę). Usługa polega zatem na tym, że Klient przekazuje Pośrednikowi Klienta bazę adresów e-mail w celu wysłania wiadomości e-mail marketingowych. Jednocześnie Klient jest administratorem danych w stosunku do przekazywanych adresów e-mail (tj. np. Klient zebrał od osób, których dane dotyczą, zgody na przesyłanie informacji handlowych drogą elektroniczną). Pośrednik Klienta pełni rolę kontrahenta odpowiedzialnego za techniczny aspekt wysyłki wiadomości e-mail marketingowych. W takim schemacie, z punktu widzenia przepisów RODO, Pośrednika Klienta uznać należy za podmiot przetwarzający (procesor) w imieniu Klienta.

Więcej wątpliwości wzbudza natomiast status poszczególnych podmiotów w bardziej złożonych relacjach związanych z prowadzeniem działań e-mail marketingowych. Relacja taka wyglądać może

w sposób następujący: **Klient** – **Pośrednik Klienta** – **Pośrednik Wydawcy (Pośrednik Dysponenta Bazy)** – **Wydawca (Dysponent Bazy).** Dotyczy to w szczególności sytuacji, kiedy **Klient nie dysponuje zasobami bazodanowymi umożliwiającymi mu dotarcie ze swoją informacją handlową do szerszego katalogu odbiorców** (brak własnej bazy adresów e-mail) i w tym celu korzysta z podmiotu zapewniającego mu wsparcie w tym zakresie. W ocenie autorów **typowy status prawny** tych podmiotów przedstawia się w sposób opisany poniżej.

Wydawca (Dysponent Bazy)

Wydawca (Dysponent Bazy) jest w opisanym procesie podmiotem, **na rzecz którego została wyrażona zgoda na wysyłkę informacji handlowej drogą elektroniczną lub komunikacji marketingowej** pochodzącej od administratora lub od podmiotów trzecich i który **posiada podstawę prawną do przetwarzania danych osobowych w celu promocji towarów i usług podmiotów trzecich**. Dysponent Bazy posiada dane umożliwiające mu wysłanie mailingu do odpowiednich segmentów odbiorców. Posiada on zatem nie tylko dane w postaci adresu e-mail, ale często również informacje dotyczące kategorii wiekowej czy geolokalizacji. Dysponent Bazy posiada pełne władztwo w procesie przetwarzania danych osobowych, podejmuje we własnym imieniu i na własną rzecz decyzje o procesach przetwarzania – o tym, w jakim celu i w jaki sposób dane są przetwarzane. **Dysponent Bazy posiada kontrolę nad działaniami decyzyjnymi (może np. wykluczyć dany adres e-mail z wysyłki marketingowej)**. Jest również podmiotem właściwym do rozpatrywania wniosków osób, których dane dotyczą, o których mowa w rozdziale III RODO. **Dysponent Bazy jest więc w omawianym procesie administratorem danych.**

Klient (Reklamodawca)

Klient zleca przeprowadzenie kampanii e-mail marketingowej i dostarcza treść wiadomości handlowej (tj. kreację), która ma być wysłana. **Nie decyduje, na które konkretnie adresy e-mail kierowany będzie mailing, określa jedynie segmenty odbiorców** (np. jego celem jest, aby e-mail trafił do mężczyzn w wieku 30-50 lat, mieszkających w ośrodkach miejskich powyżej 500 tys. mieszkańców). W takim układzie to Dysponent Bazy decyduje, na które konkretnie adresy e-mail zostanie wysłana wiadomość. Klient nie ma dostępu do danych osobowych, nie decyduje o celach i sposobach przetwarzania. Dysponent Bazy (lub Pośrednik Dysponenta) oferuje Klientowi jedynie usługę wysyłki dostarczenia kreacji do kręgu określonych kategorii odbiorców.

W opinii autorów, w takiej sytuacji – co do zasady – **uznać należy, że Klient nie jest w ramach opisanego procesu ani administratorem, ani podmiotem przetwarzającym (procesorem) bazy adresów e-mail – mówiąc inaczej** – **nie jest podmiotem, do którego w ramach opisanej kwestii stosuje się przepisy RODO.**

Klient (Reklamodawca) – Dysponent Bazy – wątpliwości interpretacyjne

W praktyce można się również spotkać z opinią, że w opisanej powyżej sytuacji to Klient jest administratorem, a Dysponent Bazy podmiotem przetwarzającym w imieniu Klienta. **Zwolennicy takiego stanowiska podnoszą, że gdyby nie zlecenie Klienta odnośnie wysłania wiadomości, dane osobowe z zasobu Dysponenta Bazy nie byłyby przetwarzane** (tj. na adresy e-mail nie byłby wysłany mailing reklamowy z kreacją konkretnego Klienta). Wskazują ponadto, że Klient określa, do jakiego segmentu odbiorców ma zostać wysłany mailing marketingowy. W konsekwencji czynności te uznają za „ustalanie celów i sposobów przetwarzania", czyniąc z Klienta administratora danych. Zwolennicy tego podejścia wskazują na decyzję GIODO (obecnie: PUODO) z dnia 19 sierpnia 2008 r. (DIS/DEC – 487/21468, 21472/08), w której GIODO uznał za administratora danych spółkę, która podjęła decyzję o organizacji loterii promocyjnej nie zaś spółkę, która faktycznie organizowała i obsługiwała tę loterię.

W opinii autorów doszukiwanie się analogii pomiędzy przetwarzaniem danych w celu organizacji loterii a przetwarzaniem danych związanym z realizacją mailingu jest jednak nietrafne. Czym innym jest bowiem powierzenie organizacji loterii i zbierania danych, a czym innym zlecenie wysyłki wiadomości

marketingowych do określonego – dość ogólnie – segmentu odbiorców. Zdaniem autorów przyjęcie koncepcji, że Klient zlecający realizację działań mailingowych jest administratorem danych niesie ze sobą wiele trudnych do odpowiedzi pytań.

Po pierwsze, Dysponent Bazy posiada – najczęściej – jedynie podstawę prawną do przetwarzania danych w celu marketingu podmiotów trzecich, nie zaś do udostępnienia tych danych (pod czym autorzy rozumieją przekazanie danych w relacji administrator – administrator) podmiotom trzecim (podmiotom takim jak Klient). Wskazać przy tym należy, że cel w postaci marketingu podmiotów trzecich jest uznawany m.in. przez GIODO (obecnie: PUODO) jako oddzielny cel przetwarzania[21]. Wyodrębnienie tego celu już samo w sobie wskazuje, że promowanie towarów i usług innych podmiotów nie czyni z nich automatycznie administratorów danych.

Przyjęcie koncepcji, że Klient jest administratorem, wiąże się z postawieniem pytania o jego podstawę prawną do przetwarzania tego rodzaju danych. Z racji braku zgody udzielonej Klientowi, musiałby to być art. 6 ust. 1 lit. f RODO (tzw. prawnie uzasadniony interes), co z kolei prowadzi do dalszych trudności, odnoszących się do tego, jak Klient miałby przeprowadzić test równowagi, nie mając dostępu do danych i nie znając nawet ich zakresu. Jak również miałby ująć ten proces w rejestrze czynności przetwarzania – o którym mowa w art. 30 ust. 1 RODO. Równie wątpliwa byłaby podstawa prawna do udostępnienia danych przez Dysponenta Bazy. W tym przypadku również należałoby opierać się na art. 6 ust. 1 lit. f) RODO, co w opinii autorów wydaje się równie kontrowersyjne.

Po drugie, przyjęcie konstrukcji, że Klient jest administratorem, sprawiałoby również problemy praktyczne. Jak bowiem Klient miałby realizować uprawnienia osób, których dane dotyczą, o których mowa w rozdziale III RODO? Istotą świadczonej usługi jest bowiem to, że Klient na żadnym etapie nie ma dostępu do danych osób, do których kierowany jest mailing. W stopce wysyłanej wiadomości jako podmiot właściwy do rozpatrywania ewentualnych reklamacji jest najczęściej wskazywany Dysponent Bazy – posiada on bowiem wszelkie informacje, aby takie reklamacje rozpatrywać. Nawet na etapie, gdy reklamacja spływa wprost do Klienta, nie otrzymuje on od Dysponenta Bazy danych pozwalających mu na udzielenie odpowiedzi, a jedynie wskazuje takiej osobie, że właściwym adresatem wniosku powinien być właśnie Dysponent Bazy. Z biznesowego punktu widzenia nie do zaakceptowania byłaby sytuacja, w której – w związku z realizacją zlecenia – Klientowi byłyby przekazywane adresy e-mail osób, do których kierowany jest mailing. W praktyce umowy zawierałyby postanowienia, z których wynikałoby, że Klient nie będzie otrzymywać od Dysponenta Bazy danych osobowych. Rodzi to z kolei pytanie, czy jeżeli uznać Klienta za administratora danych, takie postanowienia nie byłby jednak sprzeczne z RODO.

Reasumując, w ocenie autorów określanie statusu Klienta i Dysponenta Bazy na podstawie wskazywanej wcześniej decyzji GIODO z dnia 19 sierpnia 2008 r. jest nietrafne. Zapadła ona bowiem w odmiennym stanie faktycznym, w tym zanim wydana została jeszcze opinia z 16.02.2010 nr 1/2010 Grupy Roboczej Art. 29 w sprawie pojęć „administrator danych" i „przetwarzający", a w której to opinii wskazano m.in., że dla oceny, czy podmiot jest administratorem danych, istotny jest „**poziom faktycznej kontroli**"[22]. W analizowanym przypadku faktyczną kontrolę nad procesem przetwarzania danych sprawuje Dysponent Bazy, a nie Klient. Na koniec wskazać należy, że pogląd, zgodnie z którym **Klient nie jest w związku z realizacją opisywanej usługi administratorem**, został zaakceptowany przez GIODO, który w decyzji z dnia 4 kwietnia 2013 r. (DOLiS/DEC-388/13/21087,21090,21093,21094, 21095) nie dopatrzył się, aby Klienci – na zlecenie których Dysponent Bazy realizował e-mailing, bez udostępniania danych tym podmiotom – byli administratorami danych odbiorców mailingu. Ufać należy, że regulator (PUODO) dokona ostatecznego wyjaśnienia statusu prawnego Klienta (Reklamodawcy) oraz Dysponenta Bazy, kwestia ta ma bowiem kluczowe znaczenie dla sposobu funkcjonowania rynku usług e-mailingowych.

[21] Patrz np. zestawienie wyników sprawdzeń zgodności przetwarzania danych z przepisami o ochronie danych osobowych, które zostały przeprowadzone przez administratorów bezpieczeństwa informacji w bankach w zakresie marketingu kierowanego do klientów oraz osób niebędących klientami banków, Warszawa 2017, dostępne pod adresem: https://www.giodo.gov.pl/1520252/id_art/9848/j/pl

[22] Opinia nr 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" 16.02.2010, WP 169 s. 13.

E-mail marketing – status pośredników

Tak jak wyżej wskazano, najczęściej pomiędzy Wydawcą (Dysponentem Bazy) a Klientem funkcjonuje szereg pośredników, działających w imieniu Dysponenta Bazy lub Klienta. Ich status prawny, w typowych relacjach, przedstawia się zdaniem autorów w opisany poniżej sposób.

Pośrednik Wydawcy (Pośrednik Dysponenta Bazy)

Dysponent Bazy, posiadając podstawę prawną do przetwarzania danych osobowych w celu marketingu podmiotów trzecich, może powierzyć na podstawie umowy powierzenia, zgodnej z art. 28 ust. 3 RODO, przetwarzanie danych, tj. np. adresów e-mail, innemu podmiotowi (Pośrednikowi Dysponenta Bazy). Ten ostatni podmiot pełni w tym procesie rolę podmiotu przetwarzającego dane osobowe w imieniu i na zlecenie Dysponenta Bazy. Najwięcej wątpliwości w związku z tym zagadnieniem wywołuje określenie zakresu swobody działania podmiotu przetwarzającego.

Zgodnie z opinią 1/2010 Grupy Roboczej Art. 29 podmiotowi przetwarzającemu może być pozostawiony pewien margines działania. W szczególności podmiot przetwarzający może działać zgodnie z ogólnymi wytycznymi administratora, które dotyczą przede wszystkim celów i nie określają szczegółowo kwestii sposobów[23]. „Administrator może przekazać określenie „sposobów" przetwarzania w odniesieniu do kwestii technicznych lub organizacyjnych"[24]. Pośrednik Dysponenta nie może wykroczyć poza ww. margines działania. W praktyce, Pośrednikowi Dysponenta jest często powierzona realizacja niektórych uprawnień osób, których dane dotyczą np. odnotowywanie sprzeciwu na przetwarzanie danych w celach marketingowych (art. 21 ust. 2 RODO).

Pośrednik Dysponenta Bazy jest również często stroną umowy z Klientem. **W typowej kampanii e-mail marketingowej działa jako pośrednik, odsprzedając Klientowi lub Pośrednikowi Klienta usługę wysyłki treści do kręgu wyspecyfikowanych kategorii odbiorców, których administratorem jest Dysponent Bazy.**

Pośrednik Dysponenta pełni często rolę podmiotu kojarzącego potrzeby Klienta i zasoby Dysponenta Bazy w ramach usługi wysyłki e-mailingu marketingowego.

Pośrednik Klienta (Pośrednik Reklamodawcy)

Jeżeli chodzi natomiast o Pośrednika Klienta, to **pełni on rolę podmiotu kojarzącego potrzeby Klienta i zasoby Dysponenta Bazy w ramach usługi wysyłki e-mailingu marketingowego**. W praktyce Pośrednikowi Klienta sprzedawana jest przez Dysponenta Bazy lub Pośrednika Dysponenta Bazy usługa wysyłki dostarczonych treści do kręgu wyspecyfikowanych kategoriami odbiorców, a Pośrednik Klienta usługę tę odsprzedaje (refakturuje) Klientowi, który dostarcza ww. kreację do wysyłki.

W takim wariancie **Pośrednik Klienta** nie ma dostępu do danych, nie określa sposobów przetwarzania. Co do zasady **będzie zatem w stosunku do wykorzystywanych w e-mail marketingu adresów podmiotem, do którego w ramach opisanego procesu nie stosuje się RODO.**

W sytuacji jednak, gdy Klient pełni w ramach opisanego procesu rolę administratora (tj. np. mailing jest wysyłany do bazy jego klientów), wówczas Pośrednik Klienta może pełnić rolę podmiotu przetwarzającego dane osobowe na zlecenie Klienta (art. 28 ust. 3 RODO).

[23] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", 16.02.2010, WP 169 s. 14-15.

[24] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", 16.02.2010, WP 169 s. 16.

Podsumowanie

Ustalenie statusu poszczególnych podmiotów (potencjalnie) przetwarzających dane w procesie dostarczania „tradycyjnej" reklamy internetowej budzi istotne wątpliwości i z pewnością będzie się jeszcze kształtować w toku wykładni organu nadzoru, Europejskiej Rady Ochrony Danych i orzecznictwa sądów.

W związku z tym podkreślić należy, że przy dokonywaniu tej oceny kluczowa powinna być szczegółowa analiza, czy – i w jakim zakresie – podmioty te mają faktyczne władztwo na celami i sposobami przetwarzania danych osobowych, wykorzystywanych w kampanii reklamowej.

Katarzyna Ksionek
starszy prawnik,
Grupa Wirtualna Polska

Ewa Nitkiewicz
starszy prawnik,
specjalista
w Grupie RAS Polska

PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W REKLAMIE INTERNETOWEJ

Operacje przetwarzania danych osobowych na potrzeby dostosowania (personalizacji) reklamy do zainteresowań i potrzeb użytkowników wymagają odpowiedniej podstawy prawnej przetwarzania. Na każdym uczestniku rynku reklamy, w tym rynku reklamy *programmatic*, biorącym udział w spersonalizowanej kampanii reklamowej i będącym administratorem danych osobowych, spoczywa obowiązek dokonania wyboru odpowiedniej podstawy prawnej, np. zgody podmiotu danych osobowych (w modelu *opt-in*) lub prawnie uzasadnionego interesu administratora (w modelu *opt-out*). Przyjęcie zgody jako podstawy przetwarzania wymaga, aby użytkownik, będący odbiorcą spersonalizowanej reklamy internetowej, aktywnie „zdecydował się" (*opt-in*) na wykorzystanie jego danych w celach marketingowych przez uczestników rynku reklamy.

Ponadto, w przypadku niektórych działań reklamowych w internecie, legalność prowadzenia kampanii marketingowych wymaga spełnienia warunków określonych w innych niż RODO aktach prawnych, w szczególności w ustawie o świadczeniu usług drogą elektroniczną oraz Prawie Telekomunikacyjnym.

Rolą wydawcy na rynku reklamy jest informowanie użytkowników o tym, jakie ich dane, w jakim celu, na jakiej podstawie, jak długo i przez kogo będą przetwarzane, komu będą udostępniane. Oznacza to realizację obowiązków informacyjnych oraz umożliwienie wyrażenia zgody na cele marketingowe, w tym niezbędną analitykę, profilowanie, dla zaufanych partnerów wydawcy. Wydawcy są bowiem podmiotami wchodzącymi w bezpośrednią interakcję z użytkownikami, będącymi odbiorcami reklamy internetowej (zarówno bezpośredniej, jak i programatycznej) podmiotami, których użytkownicy „odwiedzają" w internecie, na stronach, a także w aplikacjach, łatwo ich identyfikują i którzy zapewniają pełną przejrzystość w procesie przetwarzania danych osobowych użytkowników w celu personalizacji reklamy internetowej.

Uzasadniony interes administratora – marketing bezpośredni

W branży internetowej, w celach marketingowych własnych i cudzych, jedną z podstaw przetwarzania danych osobowych użytkowników serwisów internetowych, jest prawnie uzasadniony interes administratora lub strony trzeciej – najczęściej wydawcy serwisów internetowych lub strony reklamodawcy (art. 6 ust. 1 lit. f) RODO). Zgodnie z motywem 47 preambuły RODO, za taki uzasadniony interes uznaje się **marketing bezpośredni**.

Marketing bezpośredni, w tym profilowanie czy niezbędna analityka, jako uzasadniony interes administratora danych osobowych, nie może być nadrzędny wobec podstawowych praw i wolności podmiotu danych. Aby zbadać, czy w określonym kontekście tak jest, administrator przeprowadza **test równowagi**. Test taki pozwala zweryfikować, czy interes administratora jest konkretny, rzeczywisty, zgodny z prawem. Ocenia obiektywnie, czy użytkownik **ma rozsądne przesłanki, aby spodziewać się przetwarzania jego danych osobowych w celu marketingowym**, np. dopasowania reklamy do jego aktywności w serwisach, w aplikacjach mobilnych, dokonanych zakupów online, czytania treści o określonej tematyce. Ważnym elementem testu równowagi jest ocena **zapewnienia użytkownikowi skutecznej realizacji prawa sprzeciwu** wobec przetwarzania jego danych osobowych w celu marketingu bezpośredniego z profilowaniem.

Wydawcy serwisów internetowych podejmują wysiłki, aby w **zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie**, udzielić swoim użytkownikowi niezbędnych informacji o przetwarzaniu

jego danych osobowych. Informacje są sformułowane **jasnym, prostym językiem, wyróżnione** w politykach prywatności, **łatwo dostępne**, a także **prezentowane graficznie,** np. jako infografiki.

Administratorzy chcą, aby użytkownik był jak najlepiej poinformowany o przetwarzaniu jego danych osobowych. Chcą, aby spodziewał się przetwarzania jego danych w celu marketingowym, rozumiał proces dopasowania reklam, treści, a także by mógł się temu skutecznie sprzeciwić.

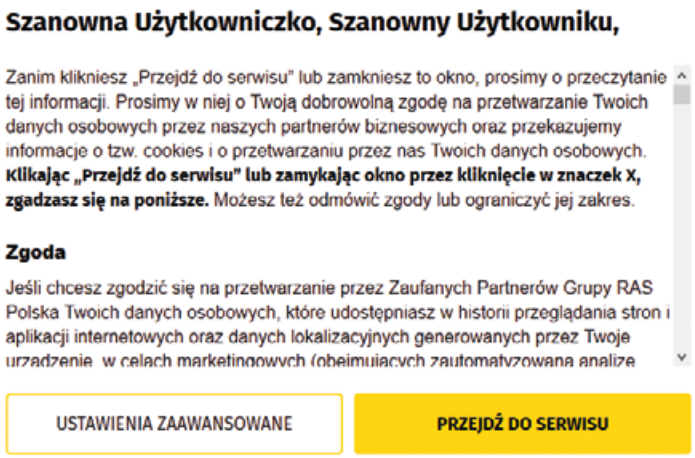
Zgoda jako podstawa przetwarzania danych osobowych w online marketingu

Zgoda stanowi kolejną podstawę przetwarzania danych użytkowników usług internetowych, w szczególności dla podmiotów, które nie mogą oprzeć przetwarzania w celu marketingowym na swoim uzasadnionym interesie.

Wyzwaniem, przed jakim stanęli wydawcy, było zaprezentowanie uczestników rynku reklamy *programmatic* i ich roli w sposób przejrzysty, tak aby użytkownik nie był „zaskoczony" tym, że jego aktywność w sieci internet, a także w aplikacjach mobilnych, i inne dane, które go dotyczą, będą wykorzystywane przez szereg podmiotów w celu skierowania do tego użytkownika spersonalizowanej reklamy. „Wydawcy stosują różne rozwiązania, aby w jasny przejrzysty sposób przekazać użytkownikom ww. informacje, m.in. stosują „okienka informacyjne", plansze informacyjne, wskazujące nazwy firm Zaufanych Partnerów, niektórzy prezentują listy Zaufanych Partnerów wraz z linkami do ich polityk prywatności, inni wspierają wdrożenie mechanizmu *open source* udostępnionego w ramach Transparency & Consent Framework (TCF)".

8. Przykład informacji o ochronie danych osobowych

Z powyżej wskazanych względów, od 25 maja 2018 r. na stronach internetowych i w aplikacjach mobilnych wydawców pojawiły się informacje o możliwości wyrażenia zgody na przetwarzanie danych osobowych użytkownika w celach marketingowych zaufanych partnerów wydawcy, zwane „**chmurkami RODO”**, „planszami RODO”, „mechanizmami zgód RODO” itp., udostępniając *de facto* platformę zarządzania zgodami CMP.



9. Przykład informacji o możliwości wyrażenia zgody na przetwarzanie danych osobowych użytkownika w celach marketingowych zaufanych partnerów wydawcy

Na potrzeby zbierania, przechowywania i cofania zgód użytkowników, na działania uczestników rynku reklamy, w szczególności reklamy *programmatic,* w sposób zapewniający przejrzystość, wydawcy wykorzystują rozwiązania technologiczne, tzw. CMP, czyli *Consent Management Platforms.* Rolą CMP jest zebranie i przechowywanie zgód oraz wygodne zarządzanie nimi przez użytkownika.

Niektórzy wydawcy samodzielnie zaprojektowali i wdrożyli indywidualne rozwiązania technologiczne tzw. CMP, czyli *Consent Management Platforms.* Część wydawców wybrała natomiast istniejące gotowe narzędzia CMP. W konsekwencji na rynku funkcjonują następujące rodzaje rozwiązań:

- narzędzia własne wydawców lub reklamodawców;
- narzędzia komercyjne, udostępniane przez firmy technologiczne,
- narzędzia firm dostarczających kompleksowe platformy adtech.

Rynek narzędzi CMP jest stale na etapie rozwoju, a wydawcy portali internetowych, serwisów społecznościowych i informacyjnych zazwyczaj korzystają z własnych CMP umożliwiających kompleksowe obsłużenie ich obowiązków w zakresie przetwarzania danych osobowych zgodnie z wymogami RODO.

Komunikat zawarty w ramach c*onsent-wall* wydawcy zazwyczaj zawiera szeroką informację o procesach, jakie zachodzą wobec danych osobowych użytkowników oraz zasadach działania rynku *programmatic,* a także informację o przetwarzaniu danych na potrzeby usług samego wydawcy i w innych celach, które wydawca chce osiągnąć, wykorzystując dane osobowe użytkowników. W praktyce często spotkać można jednak komunikaty o prostej strukturze, serwujące użytkownikom wyłącznie podstawowe informacje o korzystaniu z ich danych w celu personalizacji reklam.

Zgoda aktywna *opt-in*

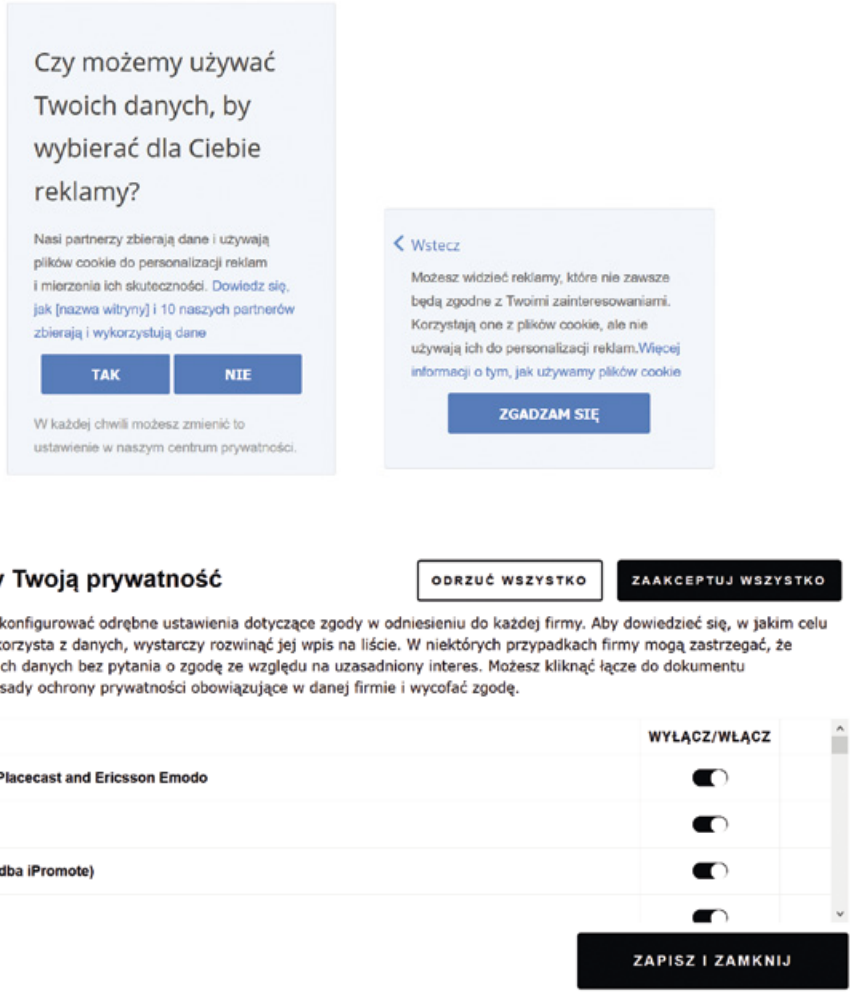
Poniższe przykłady[25] obrazują różne sposoby zbierania zgody (w modelu *opt-in*) uwzględniające wytyczne i wymagania dotyczące interfejsu użytkownika oraz UX (*user experience*, z ang. doświadczenia użytkownika), czyli wrażeń, jakich doświadcza użytkownik podczas wyrażania zgody.

[25] https://www.quantcast.com/gdpr/; https://support.cookiebot.com/hc/en-us/articles/360007652694-Cookiebot-and-the-IAB-Consent-Framework; https://www.cookiechoices.org/

Model *opt-in* musi przewidywać aktywne działanie użytkownika, którego dane mają być wykorzystane na potrzeby reklamy internetowej. Tym samym wydawca zwraca się do użytkownika, aby ten „zdecydował się", czy chce otrzymywać spersonalizowane reklamy, poprzez wykonanie określonej akcji. Wydawcy wskazują użytkownikom, jaka akcja musi zostać podjęta, jaki ruch użytkownika jest niezbędny dla wyrażenia zgody, np. kliknięcie pola wskazanego w komunikacie, przesunięcie paska, scrollowanie, zamknięcie komunikatu, kliknięcie na elementy witryny poza komunikatem. Wydawcy dokonują bieżącej oceny, na ile zapewnione są jasne informacje i na ile jasne jest dla użytkownika, że dana akcja oznacza jego zgodę w odpowiedzi na konkretne zapytanie wydawcy. Użytkownicy, których dane dotyczą, muszą być w stanie wycofać zgodę tak łatwo, jak ją wyrazili. Wydawca musi być w stanie wykazać, że zgodę uzyskano w sposób opisany powyżej i że nie została cofnięta.

Warstwy komunikatów zawierających zgody (*consent-wall*)

Pierwsza warstwa komunikatu ze zgodą (*consent-wall*):



10. Przykład pierwszej warstwy komunikatu ze zgodą (*consent-wall*)

Dobrowolność zgody ocenia się, w jak największym stopniu uwzględniając, „czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy" (art. 7 ust .4 w zw. z motywem 43 RODO).

Komunikaty zawierają proste instrukcje wskazujące użytkownikom, jak nie wyrazić zgody, jak zmienić jej zakres, np. dla poszczególnych zaufanych partnerów, **jak wycofać zgodę**. Usługi internetowe są świadczone użytkownikowi przez wydawców, bez względu na wyrażenie przez niego zgody lub jej brak. Wszystkie informacje, w tym możliwość zmiany ustawień zgód bądź wycofanie zgód, są stale dostępne dla użytkownika o 2 kliknięcia dalej (*two taps away*) zgodnie z Wytycznymi Grupy Art. 29 na temat transparentności (17/EN WP 260 rev.01).

11. Przykład informacji o możliwości wyrażenia zgody na przetwarzanie danych osobowych użytkownika w celach marketingowych zaufanych partnerów

Aby zgoda była **świadoma,** wydawca informuje, kto jest administratorem danych osobowych, **jaki zakres danych** i **w jakim celu** będzie przetwarzany oraz o **prawie do wycofania zgody** (zgodnie z Wytycznymi Grupy Art. 29 dotyczące zgody na mocy Rozporządzenia 2016/679, 17/EN WP259 rev.01 z dnia 28.11.2017, ostatnio zmienione i przyjęte dnia 10.04.2018 r.).

Zakres danych i cele przetwarzania danych użytkownika są określone na początku informacji prezentowanej w tzw. chmurce RODO i obejmuje dane osobowe udostępniane przez użytkownika w historii przeglądania stron i aplikacji internetowych oraz dane lokalizacyjne generowane przez urządzenie użytkownika w celach marketingowych (obejmujących zautomatyzowaną analizę aktywności użytkownika na stronach internetowych i w aplikacjach w celu ustalenia jego potencjalnych zainteresowań dla dostosowania reklamy i oferty) w tym na umieszczanie znaczników internetowych (*cookies* itp.).

„Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym **celu lub w tych samych celach**. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele" (motyw 32 preambuły RODO*).*

Wydawcy stosują warstwowe informowanie o odbiorcach danych (zaufanych partnerach) – przechodząc od ogólnej do granularnej (szczegółowej) informacji. W warstwie podstawowej, dostępnej bezpośrednio np. na stronie internetowej, określona jest **kategoria podmiotów**, które będą przetwarzały dane osobowe na podstawie zgody (**partnerzy biznesowi, zaufani partnerzy**), natomiast w warstwie szczegółowej podmioty te są wymienione wraz z udostępnionym mechanizmem udzielania/wycofania zgód dla poszczególnych odbiorców danych.

Model zgody prezentowanej warstwowo (stopniowo) na potrzeby reklamy internetowej wydaje się być właściwym rozwiązaniem, dzięki któremu w kolejnych warstwach zgody użytkownik może odrębnie zapoznać się z celami przetwarzania danych osobowych oraz podmiotami z rynku *programmatic* uzyskującymi dostęp do jego danych. *Consent-wall* jest jednym z możliwych skutecznych narzędzi zbierania zgód przez podjęcie określonej aktywności indywidualnego użytkownika oraz narzędziem do prostego cofnięcia udzielonej zgody, zmianą jej zakresu.

Wspieranie IAB Transparency & Consent Framework

IAB Transparency & Consent Framework, który został opracowany w ubiegłym roku przez IAB Europe, we współpracy z wieloma podmiotami rynku internetowego, określa technologiczne ramy tego, w jaki sposób wydawcy mogą pozyskiwać i zapisywać zgody na przetwarzanie danych osobowych w określonych celach przetwarzania danych od użytkowników. Wystandaryzowany w ramach IAB Transparency & Consent Framework sposób zapisu zgód umożliwia ich transmisję (udostępnienie) zaufanym partnerom uczestniczącym w procesach marketingowych, analitycznych, personalizacji, m.in. w całym zautomatyzowanym łańcuchu dostarczania treści reklamowych użytkownikom.

Wydawcy, w ramach IAB Poland, przeprowadzili wiele testów, różnych wariantów planszy służącej do informowania użytkowników o polityce prywatności, o tym, w jaki sposób mogą wyrazić, edytować lub wycofać zgodę na przetwarzanie ich danych osobowych, tak aby **należycie spełnić obowiązek informacyjny wobec użytkowników** wynikający z przepisów RODO, a jednocześnie nie uczynić go uciążliwym dla użytkownika. Dostosowano działanie planszy do środowiska desktop, mobile, jak również aplikacji mobilnych, aby zapewnić zgodność z wymogami prawa w całym ekosystemie reklamowym, a także wprowadzono szereg zmian, m.in. w systemach reklamowych, umożliwiających odpowiednie ich działanie w zależności od zakresu zgody udzielonej przez użytkownika, dostosowując się także do sytuacji wycofania przez użytkownika zgody w każdym momencie.

IAB TCF jest przedsięwzięciem otwartym na informacje zwrotne i komentarze od wydawców, regulatorów i innych podmiotów działających na rynku internetowym, co doprowadziło do jego aktualizacji, która została opublikowana w ostatnich tygodniach jako IAB TCF 2.0.

Cookies i podobne technologie

Oprócz kwestii związanych z przetwarzaniem danych osobowych użytkowników osobnym zagadnieniem jest problem dotyczący warunków stosowania przez wydawców i dostawców usług technologii umożliwiających zapisywanie informacji na urządzeniu użytkownika i odczytywanie tych informacji – tzw. *cookies*. Działanie to regulowane jest od strony prawnej przepisami ustawy Prawo Telekomunikacyjne, a docelowo ma być także przedmiotem unijnego rozporządzenia określanego roboczo jako „ePrivacy".

Warunkiem stosowania u danego użytkownika technologii *cookies* jest co do zasady jego zgoda (nie dotyczy ona jedynie kilku wyjątkowych przypadków określanych jako *cookies* „techniczne", np. *cookie* identyfikujące zalogowanie czy związane z bezpieczeństwem usługi). Zgoda ta wyrażana może być zgodnie z przepisami Prawa Telekomunikacyjnego poprzez odpowiednie ustawienia w przeglądarce (urządzeniu końcowym) dokonane przez użytkownika po poinformowaniu go o celu korzystania z *cookies* i przedstawieniu sposobu zarządzania tą technologią na własnym urządzeniu końcowym.

Taki model komunikacji zakłada powiązanie aspektu technologicznego z faktem wykorzystania technologii w procesie przetwarzania danych osobowych użytkowników i może tym samym nieść wymierne korzyści dla użytkownika, który jest lepiej poinformowany o działaniach branży *programmatic.* Samo bowiem mnożenie komunikatów i okien na witrynach nie jest dla użytkownika czytelne.

Opisana powyżej „chmurka RODO" doskonale spełnia warunki umożliwiające wyrażenie i pozyskanie zgody na *cookies*. W jej zakresie użytkownik uzyskuje bowiem zarówno bardzo szeroką i jednocześnie czytelną informację o tym, jak działają *cookies*, do czego służą i jak są wykorzystywane przez danego wydawcę oraz szczegółową informację o tym, w jaki sposób należy dokonać zmian w ustawieniach urządzenia końcowego, by ograniczyć lub całkowicie zablokować funkcjonowanie *cookies*.

Magdalena Kogut-Czarkowska
radca prawny,
Baker McKenzie

PROFILOWANIE MARKETINGOWE JAKO SZCZEGÓLNA OPERACJA NA DANYCH OSOBOWYCH

Profilowanie – źródła prawa (Rada Europy, RODO) oraz opinia Grupy Roboczej

Profilowanie służące jako narzędzie marketingowe nie jest nowym zjawiskiem. Jednakże, przed wejściem w życie RODO, nie było ono zdefiniowane w polskiej ustawie o ochronie danych osobowych z 1997 r. ani w Dyrektywie 95/46 WE. Nie znaczy to jednak, że nie było prób podjęcia uregulowania tego zjawiska w innych aktach prawnych. Definicja oraz skierowane do państw członkowskich Rady Europy rekomendacje dotyczące profilowania pojawiły się bowiem w Rekomendacji RE z 2010 r.[26]

W tym dokumencie „tworzenie profili" oznaczało „automatyczną technikę przetwarzania danych polegającą na przypisaniu danej osobie <<profilu>> (czyli zestawu danych charakteryzujących kategorię osób, który ma zostać zastosowany w odniesieniu do danej osoby) w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw". RODO, nawiązując i inspirując się Rekomendacją Rady Europy, w art. 4 pkt 4 podjęło potrzebę sprecyzowania ram prawnych profilowania i zdefiniowało je jako „dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się". O profilowaniu wypowiedziała się również Grupa Robocza Art. 29 (obecnie funkcjonująca jako Europejska Rada Ochrony Danych Osobowych)[27]. Dokument nie ma co prawda charakteru aktu prawnego, ale może być pomocny w zrozumieniu, jak organy nadzorcze w Unii Europejskiej rozumieją profilowanie i związane z nim obowiązki.

Profilowanie w RODO – elementy definicji

Z brzmienia przepisu RODO wynika, że „profilowanie" wyznaczane jest przez trzy elementy. Po pierwsze, dochodzi do przetwarzania danych osobowych. Po drugie, przetwarzanie to przyjmuje formę zautomatyzowaną, czyli taką, w której wykorzystywane są programy komputerowe oparte na algorytmach. Warto zaznaczyć, że fakt, iż w przetwarzaniu bierze udział również człowiek, nie będzie wyłączało możliwości zakwalifikowania danej czynności jako profilowania, okoliczność ta ma natomiast znaczenie dla kwalifikowanego profilowania na potrzeby wydawania automatycznych decyzji (art. 22 RODO). Po trzecie, celem profilowania jest ocena czynników osobowych danej osoby.

Zgodnie z wytycznymi Grupy Roboczej Art. 29 zwrot „ocena" oznacza, że profilowanie powinno obejmować jakąś formę oceny lub osądu osoby. Zatem prosta klasyfikacja osób na podstawie znanych cech, takich jak: ich wiek, płeć i wzrost, niekoniecznie będzie prowadzić do profilowania w rozumieniu RODO.

Podsumowując, profilowanie to zbieranie lub analizowanie informacji o osobie, aby przydzielić ją do pewnej kategorii po to, by prognozować jej zainteresowania lub prawdopodobne zachowanie.

[26] Rekomendacja CM/Rec (2010) 13. Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili.

[27] Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, przyjęte w dniu 3 października 2017 r., ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.

Profilowanie marketingowe (art. 21 ust. 3 RODO) a profilowanie na potrzeby zautomatyzowanych decyzji (art. 22 RODO)

Wokół profilowania narosło wiele „mitów". Tymczasem należy podkreślić, że profilowanie jest formą przetwarzania danych osobowych i jako takie nie jest zakazane, choć podlega zasadom dotyczącym przetwarzania danych osobowych, określonym w RODO. Zatem, profilowanie jako takie wymaga podstawy prawnej (np. zgody osoby, której dane dotyczą, lub wykazania prawnie uzasadnionego interesu) i musi być zgodne również z innymi zasadami ochrony danych (np. w zakresie adekwatności przetwarzanych danych).

W przypadku działań marketingowych przykładami profilowania może być m.in. analizowanie historii klienta oraz dopasowywanie na tej podstawie ofert lub reklam, które będą się wyświetlały tej osobie w różnych kanałach informacyjnych. Tak działają na przykład serwisy VOD (*Video-on-Demand*). Po obejrzeniu serialu wyświetlają one listę tytułów „które mogą Ci się spodobać", w oparciu o to, jakie inne programy oglądali fani zakończonego serialu.

Z kolei portal odzieżowy może dopasowywać wyświetlane swoim użytkownikom reklamy w zależności od tego, jakie typy ubrań interesowały klienta w przeszłości. Sklepy chcą trafiać reklamą w gusta poszczególnych klientów, a istnieje małe prawdopodobieństwo, że kobieta przeglądająca głównie wyjściowe sukienki będzie zainteresowana nowościami w dziale odzieży myśliwskiej. Należy w tym miejscu zwrócić uwagę, że pomimo dość wnikliwej analizy historii czy wcześniejszych „kliknięć" użytkownika, propozycje wyświetlane przez przedsiębiorców nadal pozostają wyłącznie propozycjami. Oznacza to, że ostateczna decyzja – czy użytkownik obejrzy sugerowany serial lub czy zakupi sukienkę – w dalszym ciągu należy do niego.

Dlatego od profilowania „zwykłego", o którym mowa powyżej, należy odróżnić profilowanie kwalifikowane. To drugie związane jest z automatycznym podejmowaniem decyzji, które dodatkowo rodzi dla osoby dużo poważniejsze skutki, w tym decyzje prawne. Mowa tutaj o sytuacji, w której przedsiębiorca wdraża rozwiązanie ułatwiające selekcję kandydatów do pracy, w rezultacie czego CV kandydata zostaje automatycznie odrzucone poprzez zastosowany algorytm. Takie profilowanie prowadzi do tego, iż osoba nie nawiąże stosunku pracy z pracodawcą. Podobny „automatyzm" może mieć miejsce w szeroko rozumianej działalności bankowej. Na podstawie wniosku i wcześniej dokonanych przez użytkownika transakcji, bank (a raczej program komputerowy stworzony dla banku) odmawia

udzielenia kredytu, co może mieć poważne skutki dla sytuacji życiowej dotkniętej tą decyzją osoby. Podkreślić należy, że w obu podanych przypadkach „profilowania kwalifikowanego" mamy do czynienia z jednej strony z automatyzmem decyzji, co należy rozumieć jako brak udziału – na etapie jej podejmowania – „czynnika ludzkiego", a z drugiej strony – z istotnymi skutkami prawnymi dla podmiotów danych wyrażających się brakiem zawarcia z nimi umów. Podobny skutek miałoby również np. naliczenie przez algorytm, na podstawie sprofilowanych danych, wysokości marży kredytu.

W przypadku powyższego profilowania na potrzeby automatycznych decyzji, które rodzą dla osoby konsekwencje prawne (lub podobne), RODO wprowadza szereg dodatkowych zabezpieczeń. Najważniejszym z nich jest wprowadzenie katalogu określonych sytuacji, kiedy podejmowanie takich decyzji jest dozwolone (art. 22 ust. 1 i 2 RODO) oraz prawo podmiotu danych do zakwestionowania podjętej w ten sposób decyzji (art. 22 ust. 3 RODO). Zakazane co do zasady jest również automatyczne podejmowanie decyzji wywołujących poważne skutki w oparciu o szczególne kategorie danych np. danych o zdrowiu.

Podstawy prawne profilowania marketingowego

W działalności marketingowej obejmującej przygotowywanie spersonalizowanych ofert najczęściej spotykane jest jednak „zwykłe" profilowanie, czyli takie, które nie prowadzi do podejmowania automatycznych decyzji o istotnych dla danej osoby skutkach prawnych w powyżej przedstawionym znaczeniu. Tak też widzi tę kwestię Grupa Robocza Art. 29.[28]

W takim wypadku przedsiębiorca musi przeanalizować, jaka jest możliwa podstawa prawna dla podejmowania opisanych działań. W niektórych przypadkach podmioty z branży marketingu internetowego opierają się na tzw. prawnie uzasadnionym interesie (art. 6 ust. 1 pkt f RODO). W przypadku oparcia profilowania marketingowego na przesłance prawnie uzasadnionego interesu szczególnego znaczenia nabiera odpowiednie wykonanie tzw. testu równowagi. Wymaga on z jednej strony weryfikacji przyjęcia, że administrator danych ma **rzeczywiście uzasadniony i zgodny z prawem interes** w przetwarzaniu danych osobowych (np. na cele marketingowe), a drugiej strony **wpływu tego przetwarzania na podmiot danych osobowych.**

Warunkiem dopuszczalności przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu jest uznanie, w wyniku przeprowadzenia testu równowagi, że **interes administratora danych w przetwarzaniu danych osobowych jest co najmniej równoważny wobec praw, wolności i interesów podmiotów danych osobowych.**[29]

Dodatkowo należy pamiętać o tym, że w przypadku profilowania w oparciu o uzasadniony interes przedsiębiorcy osobie przysługuje prawo do sprzeciwu wobec profilowania, jeśli wykaże, że ma w tym nadrzędny interes. W przypadku profilowania na potrzeby marketingu bezpośredniego, prawo sprzeciwu jest bezwzględne (art. 21 ust. 3 RODO). Powyższe prawa, razem z wymogiem transparentnego informowania o zamierzonym przetwarzaniu danych osobowych, w tym profilowaniu, stanowią istotne gwarancje praw użytkowników do dysponowania swoimi danymi osobowymi.

W innych przypadkach, tj. między innymi wówczas gdy test równowagi da wynik negatywny, konieczne jest uzyskanie zgody od podmiotów danych na przetwarzanie, w tym profilowanie, ich danych osobowych na cele marketingowe (art. 6 ust. 1 pkt a RODO).

[28] W opinii 2016/679, Grupa Robocza wskazuje: „W wielu typowych przypadkach decyzja o skierowaniu do danej osoby spersonalizowanej oferty reklamowej sporządzonej na podstawie rezultatów profilowania nie będzie wywierała podobnie istotnego wpływu na osoby fizyczne (…)". Z drugiej strony, Grupa Robocza dostrzega sytuacje, w których działanie marketingowe w oparciu o profil może być poważne w skutkach, np. jeśli dotyczy różnicowania cen w oparciu o prognozowane cechy charakteru lub dotyczy osób szczególnej troski.

[29] Więcej o tej przesłance przetwarzania w opinii 06/2014 Grupy Roboczej Art. 29 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE.

OBOWIĄZEK INFORMACYJNY W ŚRODOWISKU INTERNETOWYM

Wojciech Piszewski
adwokat,
Agora S.A.

Obowiązek informacyjny w RODO – podstawowe zasady

RODO w sposób analogiczny do poprzednio obowiązującej ustawy o ochronie danych osobowych nakłada na administratorów danych osobowych obowiązki informacyjne w stosunku do podmiotów danych, tj. podmiotów, których dane zamierzają przetwarzać. Równocześnie zakres informacji, który powinien zostać przekazany podmiotowi danych na podstawie art. 13 i art. 14 RODO, został istotnie rozszerzony. Katalog tych informacji jest inny w przypadku, gdy dane osobowe pozyskiwane są od osoby, której dotyczą (art. 13 RODO), a inny gdy pozyskiwane są w odmienny sposób (art. 14 RODO). Obejmuje on w szczególności informację o celu przetwarzania danych, podstawie prawnej przetwarzania, tożsamości administratora, okresie, przez jaki dane osobowe będą przetwarzane oraz o odbiorcach danych lub kategoriach tych odbiorców. Jednocześnie **zakres informacji, które zgodnie z RODO muszą zostać przekazane podmiotowi danych, nie jest uzależniony od formy ich pozyskiwania i sposobu utrwalenia – dotyczy to zarówno tradycyjnych, „analogowych" form przetwarzania danych, jak również ich przetwarzania w środowisku cyfrowym, w tym na potrzeby reklamy internetowej.** Zatem niezależnie od tego, czy dane pozyskiwane są za pośrednictwem tradycyjnego formularza, czy też za pomocą rozwiązań technologicznych pozwalających gromadzić i przetwarzać dane o aktywności użytkowników stron internetowych (przykładowo poprzez informacje zapisywane w plikach *cookies*), zakres informacji, jaki musi trafić do osoby, której dane są przetwarzane, pozostaje taki sam.

Przekazanie określonych informacji w ramach wykonania obowiązków informacyjnych musi jednocześnie odpowiadać określonym standardom jakościowym, co ma na celu zagwarantowanie, że informacja rzeczywiście dotrze do jej odbiorcy i – co bardziej istotne – że zostanie zrozumiana (RODO kładzie szczególny nacisk na efektywność komunikacji z podmiotami danych). Standard ten, wyrażony w motywie 39 preambuły RODO oraz w treści art. 12 ust. 1 RODO, sprowadzić można do kilku podstawowych wymogów odnoszących się zarówno do wykorzystywanego języka komunikacji, jak również do sposobu jej przekazania, tj. do wymogów, aby informacje związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

Obowiązek informacyjny związany ze zbieraniem danych osobowych powinien być wykonywany z inicjatywy administratora danych, tj. bez konieczności występowania z dodatkowym żądaniem przez podmiot danych. Innymi słowy, to administrator powinien „aktywnie" zadbać o to, aby dostarczyć podmiotowi danych wszelkie wymagane przepisami informacje o przetwarzaniu danych i zapewnić, aby sposób ich przekazania odpowiadał zasadzie prostoty i jasności przekazu. W praktyce oznaczać to będzie albo udzielenie (przekazanie) niezbędnych informacji bezpośrednio przez administratora, albo skierowanie podmiotu danych do miejsca, w którym takie informacje się znajdują (np. link do strony, informacja o możliwości skorzystania z kodu QR itd.)[30].

RODO nie daje administratorom żadnych konkretnych wskazówek odnośnie treści informacji przekazywanych odbiorcom danych (m.in. jakiego języka używać; jakich słów i zwrotów unikać; czy wreszcie jak szczegółowo opisać dane zagadnienie), jak również odnośnie formy przekazywanego komunikatu (m.in. czy powinno to nastąpić w ramach polityki prywatności serwisu internetowego; czy też odrębnego bannera zawierającego zestaw wszelkich wymaganych informacji) – w tym zakresie **to administratorzy muszą samodzielnie podjąć decyzję, jak sfomułować i następnie jak „dostarczyć" wszystkie informacje wymienione w art. 13 i 14 RODO w sposób, który będzie zwięzły,**

[30] Wytyczne Grupy Roboczej Art. 29 dotyczące przejrzystości na mocy rozporządzenia 2016/679.

zrozumiały i jasny dla ich odbiorców i to administratorzy ponoszą pełną odpowiedzialność za podjęte w tym zakresie decyzje. Powyższe daje administratorom znaczny poziom swobody w doborze odpowiedniego, tj. uwzględniającego specyfikę danego procesu przetwarzania, sposobu w zakresie wykonania obowiązków informacyjnych. **Jak wskazuje Grupa Robocza Art. 29, administrator ma wręcz obowiązek uwzględnić wszelkie okoliczności związane ze zbieraniem danych w konkretnym procesie przetwarzania,** a w szczególności wziąć pod uwagę poziom doświadczenia użytkownika/pomiotu danych[31]. W praktyce oznacza to konieczność doboru środków wyrazu do rodzaju odbiorcy, co wydaje się wnioskiem dość oczywistym z punktu widzenia celu, jakim jest przecież skuteczne przekazanie informacji. Tym samym obowiązek informacyjny (sposób jego wykonania), na stronie internetowej zawierającej „lekkie" treści, np. o tematyce rozrywkowej kierowanej do młodzieży, może (a wręcz powinien) różnić się od obowiązku realizowanego na stronie internetowej dedykowanej „poważnym" tematom, np. prawnym czy gospodarczym, i kierowanej do zupełnie innej grupy odbiorców.

Sposoby spełniania obowiązku informacyjnego w internecie

Niezależnie od powyższych trudności związanych z praktyką wykonywania obowiązków informacyjnych – pozostaje jeszcze, równie istotna, kwestia wkomponowania klauzul informacyjnych w poszczególne funkcjonalności stron internetowych oraz usług świadczonych za ich pośrednictwem. Jest to szczególnie ważne w przypadku, w którym dana strona oferuje co najmniej kilka usług jednocześnie, tj. przykładowo gromadzi dane o aktywności użytkowników na potrzeby reklamy dopasowanej do ich preferencji, daje możliwość zarejestrowania się na newsletter oraz do poczty elektronicznej.

Jest dość oczywiste, iż **klauzula informacyjna powinna być „widoczna" bezpośrednio na etapie zbierania danych od podmiotu danych – co stanowi najpewniejszy sposób wypełnienia wymogów związanych z przejrzystością procesów przetwarzania.** Mianowicie – podmiot danych otrzymuje informacje bezpośrednio w momencie, gdy „zostawia" swoje dane (np. w formularzu rejestracyjnym, służącym do założenia konta poczty elektronicznej, czy przy zapisie na newsletter), co istotnie ogranicza ryzyko wprowadzenia podmiotu danych w błąd odnośnie celów i sposobów przetwarzania jego danych w konkretnych procesach.

Z tego względu **wypełnienie obowiązku informacyjnego następować powinno w sposób adekwatny do sposobu zbierania danych**, tj.:

- w przypadku zbierania danych za pośrednictwem strony WWW – należy zamieścić stosowne informacje w bezpośrednim sąsiedztwie formularza służącego do wprowadzania danych,
- w przypadku zbierania danych za pośrednictwem komunikacji e-mail lub podobnej – należy zamieścić stosowne informacje w bezpośrednim sąsiedztwie takiego oznaczenia adresu komunikacji (adres e-mail, nr komunikatora) lub w instrukcji nawiązania komunikacji,
- w przypadku reklamy internetowej realizowanej z wykorzystaniem danych gromadzonych za pomocą m.in. plików *cookies* lub innych podobnych technologii (w tym reklamy realizowanej w modelu *programmatic*), z uwagi na brak jednego konkretnego miejsca, w którym dochodzi do zbierania danych osobowych (jak w przypadku np. formularzy internetowych) – należy zamieścić odpowiednie informacje jeszcze przed rozpoczęciem korzystania ze strony internetowej. Przykładowo, informacje takie pojawić się mogą w ramach komunikatu wyświetlanego użytkownikom bezpośrednio po wejściu na danę stronę internetową.

[31] Wytyczne Grupy Roboczej Art. 29 dotyczące przejrzystości na mocy rozporządzenia 2016/679.

Obowiązki informacyjne – największe wyzwania administratorów danych osobowych

Prawidłowa realizacja obowiązku informacyjnego jest niewątpliwie jednym z kluczowych wyzwań, przed którym stają administratorzy danych osobowych. Doświadczenia wynikające z pierwszego roku stosowania RODO pokazują, iż obowiązki informacyjne wykonywane są przez administratorów bardzo różnie i niestety nie zawsze prawidłowo. Wniosek, o którym mowa, dotyczy niemalże w równym stopniu tradycyjnych form przekazywania informacji, jak również tych wykorzystywanych w świecie cyfrowym. W tym ostatnim przypadku – znaczna liczba technicznych możliwości realizacji obowiązku informacyjnego (np. za pomocą poczty elektronicznej czy wszelkiego rodzaju komunikatów pojawiających się na stronach internetowych, okienek *pop-up*, powiadomień *push* i *pull*) tylko pozornie ułatwia jego wykonanie. Jednocześnie budzi bowiem sporo wątpliwości odnośnie miejsca czy momentu, w którym powinny zostać przekazane poszczególne informacje, szczególnie wobec przyjęcia warstwowego podejścia do wykonywania obowiązków informacyjnych. Dotyczy to w szczególności procesów przetwarzania danych związanych z nowoczesną reklamą internetową, a zwłaszcza reklamą realizowaną w modelu *programmatic.*

Podkreślenia wymaga, że przekazanie informacji, zawierającej wszystkie elementy wskazane odpowiednio w art. 13 i 14 RODO, nie jest wystarczające do w pełni prawidłowego wykonania obowiązku informacyjnego. Formułowanie rozbudowanych i bardzo szczegółowych klauzul informacyjnych, których przeczytanie (od razu i w całości) jest niezbędne do tego, aby dotrzeć do treści umieszczonych na stronie internetowej czy skorzystać z dostępnej tam usługi, nie jest – wbrew często pojawiającym się opiniom – właściwym rozwiązaniem. Po pierwsze, tego rodzaju praktyka jest niewątpliwie uciążliwa dla odbiorców przekazywanych informacji i wcale nie prowadzi do założonego celu – nadmiar informacji podanych w nieprzystępnej formie i nieodpowiednim miejscu, często sformułowanych z wykorzystaniem specjalistycznego, hermetycznego języka nie zwiększa poziomu wiedzy i świadomości w zakresie procesu przetwarzania danych. **Przeciwnie – zbyt duża ilość informacji sformułowanych z pominięciem wymogów dotyczących przejrzystości i jasności przekazu prowadzić może do dezinformacji na skutek tzw. „przeładowania informacyjnego”.** Po drugie, takie podejście do wykonywania obowiązków informacyjnych utrudnia normalne korzystanie z usług społeczeństwa informacyjnego. W efekcie jest również niekorzystne z biznesowego punktu widzenia administratorów, którym zależy przecież na tworzeniu usług i produktów możliwie najbardziej atrakcyjnych i przyjaznych dla klientów. Po trzecie wreszcie, takie podejście budzić może wątpliwości natury prawnej, szczególnie w kontekście wymogów wynikających z zasady przejrzystości, tj. wymogów formułowania informacji kierowanych do podmiotów danych w sposób zwięzły i przejrzysty. Zasadę tę w odniesieniu do wykonywania obowiązków informacyjnych można by sprowadzić do dość prostej dyrektywy, tj. nakazu informowania w taki sposób, aby odbiorca zrozumiał

przekazywaną informację (czyli aby informacja „dotarła" do odbiorcy, do którego jest kierowana), a nie tak, aby tylko formalnie sprostać wszelkim wymogom związanym z przekazywaniem określonych informacji. **Bardzo istotny jest bowiem również sposób wykonania obowiązków informacyjnych, a ten powinien uwzględniać wymogi wskazane w art. 12 ust. 1 RODO, zgodnie z którym administrator powinien przekazywać informacje w zwięzłej, przejrzystej i łatwo zrozumiałej formie**.

Jak się wydaje, przyczyną wyżej wspomnianych praktycznych problemów z prawidłowym wykonaniem obowiązków informacyjnych jest konieczność pogodzenia dwóch pozornie sprzecznych ze sobą elementów, tj. z jednej strony znacznej ilości informacji, które administratorzy mają obowiązek przekazać podmiotom danych (art. 13 i 14 RODO), a z drugiej konieczności zachowania zwięzłej, przejrzystej i łatwo zrozumiałej formy przekazu (art. 12 RODO). **Rozwiązaniem w powyższym zakresie wydaje się przyjęcie, zgodnie ze stanowiskiem Grupy Roboczej Art. 29, tzw. „warstwowego podejścia" do wykonania obowiązku informacyjnego** (ang. *layer approach*). Podział wszystkich informacji, których przekazanie podmiotom danych składa się na obowiązek informacyjny, na kilka grup/zestawów oraz przekazywanie ich stopniowo (zgodnie z założeniami warstwowego podejścia) wydaje się jednocześnie odpowiadać na problem „przeładowania informacyjnego", tj. sytuacji, w której podmiot danych otrzymuje jednocześnie tak wiele szczegółowo ujętych informacji dotyczących przetwarzania jego danych osobowych, że w efekcie nie jest w stanie ich przyswoić i zrozumieć.

Warstwowe podejście do wykonania obowiązku informacyjnego

Warstwowe podejście do wykonywania obowiązków informacyjnych – rozwiązanie zaproponowane przez Grupę Roboczą Art. 29 – w możliwie największym uproszczeniu oparte jest na przekazywaniu wymaganych prawem informacji w dwóch lub w kilku płaszczyznach (poziomach) komunikacji. W środowisku cyfrowym możliwie jest zatem odesłanie do różnych kategorii informacji zamiast przekazania wszystkich informacji w pojedynczym komunikacie wyświetlanym na ekranie. Tytułem przykładu – na poziomie formularza rejestracyjnego, w ramach którego zbierane są dane osobowe, użytkownik otrzymuje podstawowe informacje o procesie przetwarzania danych (pierwsza warstwa informacyjna) i jednocześnie zostaje odesłany do polityki prywatności, w ramach której znajduje wszystkie pozostałe informacje (druga warstwa informacyjna). W zależności od stopnia skomplikowania procesu warstw informacyjnych może być również więcej – kluczowe jest jednak zachowanie językowej, logicznej i funkcjonalnej spójności pomiędzy poszczególnymi warstwami tak, aby spełniona była zasada przejrzystości przetwarzania danych. Zgodnie z wytycznymi Grupy Roboczej, w ramach pierwszej warstwy informacyjnej administrator ma obowiązek przekazać przede wszystkim informacje o (i) celach przetwarzania, (ii) tożsamości administratora danych i (iii) prawach osoby, której dane dotyczą. Chodzi zatem o te kategorie informacji, dzięki którym podmiot danych będzie w stanie zrozumieć, jakie będą konsekwencje przetwarzania jego danych osobowych w konkretnym procesie przetwarzania.

Pozostałe wymagane prawem informacje mogą znaleźć się w kolejnej warstwie informacyjnej. Z uwagi na konieczność zbudowania funkcjonalnego połączenia pomiędzy pierwszą i drugą (odpowiednio drugą i kolejną) warstwą informacyjną, konieczne jest również oczywiście jasne i niebudzące wątpliwości odesłanie do tej drugiej warstwy. Zatem, poza wyżej wymienionymi elementami treściowymi klauzuli informacyjnej, powinna się w niej znaleźć również informacja, gdzie można zapoznać się z kompletem informacji na temat przetwarzania danych osobowych.

Jakie są zalety warstwowego podejścia do wykonywania obowiązków informacyjnych? Jak wskazuje Grupa Robocza Art. 29, takie podejście pozwala uniknąć „przeładowania informacyjnego"[32], tj. sytuacji, w której odbiorca informacji, na skutek zbyt dużej ich ilości oraz mało przejrzystej formy ich przekazania przestaje rozumieć treść komunikatu lub zniechęca się do przeczytania go w całości. Dodatkowo pozwala ono w efektywny sposób pogodzić znaczny zakres informacji, jakie muszą zostać przekazane podmiotom danych, z wymogiem, aby wszystkie te informacje zostały przekazane w jasny i zrozumiały sposób. Jednocześnie Grupa Robocza Art. 29 wprost wskazuje, że właściwym rozwiązaniem jest pozostawienie podmiotom danych wyboru w zakresie tego, z którymi informacjami

[32] Wytyczne Grupy Roboczej Art. 29 dotyczące przejrzystości na mocy rozporządzenia 2016/679.

chcą się zapoznać. Ten ostatni wniosek (oparty, jak się wydaje, na oczywistym założeniu, że nikogo nie da się zmusić do przeczytania klauzuli informacyjnej) wymaga szczególnego uwypuklenia. Wobec powyższego, praktyczne rozwiązania w zakresie wykonania obowiązku informacyjnego, które w celu zapoznania się z kompletem informacji o przetwarzaniu danych, wymagają od podmiotów danych podjęcia określonych działań (przykładowo kliknięcia w „dowiedz się więcej", „zobacz listę zaufanych partnerów", wejścia w „ustawienia zaawansowane" czy „politykę prywatności") uznać należy za w pełni prawidłowe. Oczywiście administrator danych osobowych ma obowiązek zadbać o to, aby precyzyjnie i jasno wskazać, jakie konkretne działanie musi zostać podjęte w celu otrzymania kompletnej informacji o przetwarzaniu.

Ważne jest, żeby pierwsza, podstawowa warstwa obowiązku informacyjnego realizowana była w formie właściwej dla zbierania informacji w ramach danego procesu – osoba informowana powinna łatwo i przede wszystkim już w momencie gromadzenia jej danych osobowych otrzymać podstawowe informacje na temat danego procesu przetwarzania. Przekazanie informacji w warstwie szczegółowej może natomiast polegać na odesłaniu do polityki prywatności (link), a w przypadku innych – niż poprzez stronę internetową – form komunikacji może się odbywać w następujący sposób:

- w formie wiadomości e-mail przesyłanej osobie, której dane są zbierane, przygotowane do pobrania pod unikalnym adresem URL,
- w formie komunikatu na stronie WWW dostępnego tylko dla osoby, której dane są zbierane (zakładka prywatność np. w panelu konta użytkownika).

Realizacja obowiązku informacyjnego na kilku poziomach (zgodnie z wyżej opisanymi założeniami) wydaje się najbardziej odpowiednim rozwiązaniem w przypadku bardziej skomplikowanych procesów przetwarzania, np. w przypadku reklamy internetowej realizowanej w modelu *programmatic*. Poziom skomplikowania tego procesu nie pozwala bowiem na jasne i zrozumiałe dla użytkowników stron internetowych podanie wszelkich wymaganych informacji za jednym razem, przykładowo wyłącznie w ramach jednego komunikatu wyświetlanego na stronie internetowej.

Obowiązek informacyjny w marketingu internetowym

Mając na uwadze, że informacje o użytkownikach stron internetowych, które zbierane są w ramach nowoczesnego marketingu internetowego, w określonych sytuacjach mogą stanowić dane osobowe, niezbędne jest rozważenie, jak w tej sytuacji wykonać obowiązki informacyjne wobec osób, których dane te dotyczą[33]. W pierwszej kolejności należy określić, jaka będzie podstawa prawna tego obowiązku, a w konsekwencji – jaki będzie zakres informacji wymagających przekazania podmiotowi danych (czyli „co przekazać?"). Następnie konieczne będzie zastanowienie się nad praktycznymi sposobami przekazania tych informacji w taki sposób, aby sprostać wymogom art. 12 RODO, tj. aby informacje zostały przekazane w zwięzłej, przejrzystej i łatwo zrozumiałej formie (czyli „jak przekazać?").

[33] Podkreślenia wymaga, że typowe identyfikatory internetowe, np. *ID cookie*, nie stanowią „same w sobie" danych osobowych. Danymi osobowymi będą dopiero informacje gromadzone za ich pośrednictwem lub do nich przypisane. Innymi słowy, identyfikatory powinny być traktowane jako dane osobowe dopiero wówczas, gdy łączone są z innymi unikatowymi identyfikatorami lub innymi informacjami, które pozwalają na identyfikację danej osoby fizycznej.

W większości przypadków nie budzi wątpliwości określenie tego, który z obowiązków informacyjnych powinien zostać wykonany przez administratora danych przetwarzającego je w ramach usług związanych z marketingiem internetowym, tj. czy będzie to obowiązek związany ze zbieraniem informacji bezpośrednio od podmiotu danych (art. 13 RODO), czy też obowiązek wynikający z innych sposobów zbierania tych danych (art. 14 RODO). **W typowej sytuacji administrator będzie miał obowiązek wykonać obowiązek wynikający z art. 13 ust. 1 i 2 RODO – z uwagi na to, że dane osobowe będą zbierane bezpośrednio od osoby, której dotyczą** (np. od osoby odwiedzającej daną stronę internetową). W świetle wytycznych Grupy Roboczej Art. 29 za dane osobowe zbierane bezpośrednio od danej osoby uznać należy nie tylko dane „aktywnie" przekazane przez podmiot danych (przykładowo w sytuacji wypełnienia formularza rejestracyjnego), ale również dane pozyskiwane przez administratora w drodze obserwacji (np. obserwacja „aktywności" danego uczestnika strony internetowej poprzez technologie śledzące)[34].

Odnosząc się do kwestii sposobów wykonania obowiązku informacyjnego, **warstwowe podejście do jego wykonania zostało przyjęte i wdrożone przez niemal wszystkich wydawców serwisów internetowych** (oczywiście konkretne przyjęte rozwiązania różnią się w szczegółach, ale – co ważne – wszystkie oparte zostały na podobnych założeniach). Mając na uwadze fakt, iż to właśnie za pośrednictwem serwisów internetowych ich użytkownicy otrzymują informacje o przetwarzaniu ich danych osobowych dla celów nowoczesnej reklamy internetowej (w tym w szczególności reklamy realizowanej w modelu *programmatic)* – serwisy są naturalnym „miejscem kontaktu" użytkowników i wszystkich podmiotów zaangażowanych w procesie reklamowym, powyższą praktykę należy ocenić zdecydowanie pozytywnie. **Stanowi ona istotny krok w stronę zwiększenia przejrzystości całego procesu przetwarzania danych osobowych w celu wyświetlania reklam i treści dopasowanych do preferencji użytkowników.**

Podkreślenia wymaga, że wydawcy stanęli przed szczególnie trudnym wyzwaniem w związku ze sposobem funkcjonowania rynku reklamy *programmatic*, który angażuje w proces przetwarzania danych bardzo wiele podmiotów występujących w bardzo różnych rolach (reklamodawcy, platformy popytowe i podażowe, domy mediowe oraz inni pośrednicy reklamowi). Ich zadaniem było zatem zaprojektowanie poszczególnych warstw zawierających informacje o przetwarzaniu danych w taki sposób, aby użytkownik danego serwisu od samego początku, tj. od chwili wyświetlenia danej strony internetowej miał pełną i jednocześnie jasną informację zarówno o podmiotach, które biorą udział w procesie przetwarzania, jak i o celach przetwarzania prowadzącego do dopasowania treści serwisu lub personalizacji wyświetlanej na jego powierzchni reklamy.

W tym celu wydawcy serwisów internetowych zdecydowali się wykorzystać tzw. *consent- walls*, tj. **specjalne plansze wyświetlane użytkownikom od razu po wejściu na daną stronę internetową, umożliwiające również wyrażenie zgody na przetwarzanie danych osobowych w celach prowadzenia reklamy internetowej opartej na analizie danych dotyczących „aktywności" użytkowników i/lub wyrażenie zgody na instalowanie plików *cookies* oraz wykorzystywanie informacji w nich zapisanych m.in. do celów marketingowych (zgodnie z przepisem art. 173 Prawa Telekomunikacyjnego).** *Consent-walls*, obok funkcjonalności związanych z wyrażeniem zgody, stanowią jednocześnie pierwszą warstwę w ramach wykonania obowiązku informacyjnego i zawierają najbardziej istotne informacje o procesie przetwarzania danych. Zazwyczaj są to informacje (i) mówiące o celu przetwarzania danych (dopasowywanie treści oraz personalizacja wyświetlanych reklam), (ii) kategorii wykorzystywanych danych (dane o „aktywności" użytkownika zapisywane w plikach *cookies*) oraz (iii) podmiotach zaangażowanych w proces przetwarzania (tu najczęściej pojawia się określenie „zaufani partnerzy"). Dodatkowo w ramach tej pierwszej warstwy znajduje się zwykle odesłanie do polityki prywatności lub innego miejsca, w którym podmiot danych może uzyskać komplet informacji na temat przetwarzania jego danych osobowych.

Zatem, użytkownikowi wchodzącemu na stronę internetową wyświetlany jest komunikat zawierający podstawowe informacje o przetwarzaniu jego danych osobowych (pierwsza warstwa obowiązku informacyjnego), a jednocześnie zawarty w nim zwrot „zobacz więcej" czy „dowiedz się

[34] Wytyczne Grupy Roboczej Art. 29 dotyczące przejrzystości na mocy rozporządzenia 2016/679.

więcej" stanowi aktywny link odsyłający do dokumentu, w którym proces przetwarzania został opisany kompletnie, tj. zgodnie z art. 13 ust. 1 i 2 RODO (druga warstwa obowiązku informacyjnego).

Z perspektywy administratora będącego wydawcą, tj. właścicielem strony internetowej, na którą wprowadzone zostały technicznie rozwiązania pozwalające na instalowanie technologii umożliwiających gromadzenie danych o użytkownikach stron internetowych, w szczególności zapisywanie ich w plikach *cookies* – najprostszym i najbardziej intuicyjnym rozwiązaniem wydaje się być zrealizowanie obowiązków informacyjnych w pełnym zakresie właśnie w polityce prywatności.

W ramach projektowania powyższych rozwiązań wydawcy stron internetowych przejęli dwa zasadnicze modele działania, tj.:

- wykorzystali stosowane jeszcze przed RODO komunikaty zawierające klauzulę zgody na przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym użytkownika końcowego (czyli potocznie „zgoda na pliki *cookies*"), uzupełniając je o klauzulę zgody na przetwarzania danych osobowych oraz pierwszą warstwę informacji o procesach przetwarzania danych osobowych,
- stworzyli nowe komunikaty obok równolegle istniejących komunikatów ze zgodą na pliki *cookies*, zawierające tylko zgodę na przetwarzania danych osobowych oraz pierwszą warstwę informacji o procesach przetwarzania.

Mając na uwadze wytyczne wynikające z zasady przejrzystości (jednej z podstawowych zasad wynikających z RODO), bardziej prawidłowe wydaje się pierwsze rozwiązanie. Połącznie obu klauzul zgody w jednym komunikacie od razu wskazuje na powiązanie pomiędzy instalowaniem plików *cookies* a przetwarzaniem danych osobowych w nich zapisanych (tj. przykładowo informacji o „aktywnościach" danego użytkownika na stronie internetowej), tym samym dając użytkownikowi podstawową wiedzę na temat sposobu funkcjonowania reklamy internetowej. Dodatkowo, mniejsza liczba komunikatów i zawartych w nich informacji jest po prostu bardziej czytelna i przyjazna dla użytkownika.

Tytułem przykładu, treść wyżej wspominanego *consent-wall* w zakresie wykonania obowiązku informacyjnego dotyczącego przetwarzania danych osobowych może wyglądać następująco: „poprzez (…) wyrażasz zgodę na przetwarzanie danych osobowych przez X oraz **Zaufanych Partnerów X** do celów marketingowych, w szczególności na potrzeby wyświetlania reklam dopasowanych do Twoich zainteresowań i preferencji (…). Pamiętaj, że wyrażenie zgody jest dobrowolne, a wyrażoną zgodę możesz w każdej chwili cofnąć. **Dowiedz się więcej lub zdecyduj o zgodzie".**

W oparciu o dotychczasowe doświadczenia w stosowaniu RODO oraz wyżej poczynione uwagi dotyczące standardów komunikacji z podmiotami danych osobowych, tak zaprojektowany sposób wypełnienia obowiązku informacyjnego powinien spełniać następujące wymogi:

- *consent-wall* powinien być czytelnie wyodrębniony od pozostałej zawartości strony internetowej (tak aby nie został przypadkowo „pominięty"), a informacje w nim zawarte dobrze widoczne dla użytkowników,
- komunikat w nim zawarty powinien być sformułowany w sposób możliwie jasny i precyzyjny, tj. z wykorzystaniem krótkich zdań i powszechnie zrozumiałego, potocznego języka, a jednocześnie powinien zawierać podstawowe informacje o procesie przetwarzania (cel, tożsamość administratora oraz kategorie podmiotów zaangażowanych w przetwarzanie danych),
- komunikat nie powinien być zbyt długi i zawierać zbyt szczegółowych informacji – te są przecież zawarte w drugiej warstwie informacyjnej, czyli w polityce prywatności, w szczególności komunikat nie powinien wymieniać wszystkich odbiorców danych występujących w modelu reklamy *programmatic*, a jedynie kategorię tych odbiorców (rozwiązanie wprost dopuszczane w treści art. 13 ust. 1 pkt e RODO),
- komunikat powinien również zawierać krótkie wyjaśnienie, sformułowane potocznym językiem, co do tego, jakie będą konsekwencje przetwarzania danych osobowych użytkownika,

- komunikat powinien zawierać widoczne odesłanie do miejsca, w którym zawarte są wszystkie informacje o procesie przetwarzania danych, np. do polityki prywatności,
- polityka prywatności powinna zawierać wszystkie informacje wymienione w art. 13 ust. 1 i 2 RODO, a jednocześnie być sformułowana jasnym, prostym i zrozumiałym językiem,
- polityka prywatności musi być łatwo dostępna na każdym etapie korzystania ze strony internetowej, a nie tylko przez odesłanie z komunikatu zawartego w *consent-wall*. W tym zakresie polityka prywatności powinna być co najmniej podlinkowana w dolnej części każdej strony danego serwisu,
- komunikat zawarty w *consent-wall* nie powinien nadmiernie utrudniać normalnego korzystania z danego serwisu i jego funkcjonalności, w szczególności to użytkownik powinien samodzielnie decydować o tym, kiedy zapozna się z informacjami o przetwarzaniu jego danych osobowych.

Podsumowanie

Należy pozytywnie ocenić fakt, że wydawcy serwisów internetowych zdecydowali się na warstwowe podejście do wykonania obowiązków informacyjnych wynikających z RODO. **Wobec znacznego poziomu skomplikowania procesów przetwarzania danych, związanych z reklamą internetową,** a w szczególności tą realizowaną w modelu *programmatic,* to właśnie ten sposób przybliżenia wskazanych wyżej procesów użytkownikom serwisów należy uznać za właściwy, tj. odpowiednio prosty oraz czytelny. Jednocześnie należy zakładać, że przyjęte rozwiązania będą podlegać dalszym modyfikacjom i ujednoliceniu w ramach inicjatyw branżowych – w szczególności w ramach opracowanego przez IAB Europe standardu IAB Transparency & Consent Framework.

REALIZACJA PRAW PODMIOTÓW DANYCH W INTERNECIE

Żaneta Sadowska
inspektor ochrony danych, Grupa ZPR Media

Magdalena Tomaszewska
radca prawny, inspektor ochrony danych, Grupa naTemat

Żądania osób, których dane dotyczą – zakres uprawnień w RODO

RODO zachęca do skorzystania z realizacji praw przez wszelkie podmioty danych, a więc także te, których dane są przetwarzane przez podmioty z branży internetowej. Takimi podmiotami praw są np. użytkownicy internetu, którzy: przeglądają strony internetowe, korzystają z usług skrzynek pocztowych, dokonują zakupów w sklepach internetowych, biorą udział w konkursach ogłaszanych na stronach internetowych czy też wypowiadają się na stronach portali czy w serwisach społecznościowych. W związku z tym powstała konieczność stworzenia procedury umożliwiającej wystąpienie przez danego użytkownika z odpowiednim żądaniem do danego podmiotu z branży internetowej. Grupa Wdrożeniowa GDPR IAB Europe opracowała dokument roboczy odnoszący się do żądań podmiotów danych[35] celem wskazania wytycznych w tym zakresie. Dokument ten pokazuje, w jaki sposób użytkownicy internetu mogą skorzystać z przysługujących im praw.

Procedura realizacji praw dotyczy wszystkich uprawnień zagwarantowanych w art. 12-22 RODO, motywach 39, 58-72, 166 i 167 preambuły RODO oraz art. 3-5 uodo. Procedura realizacji praw podmiotów danych powinna w szczególności określać zasady postępowania dotyczące rozpatrywania następujących rodzajów żądań podmiotów w zakresie realizacji ich uprawnień:

- prawa dostępu do informacji, w tym prawa do kopii danych (art. 15),
- prawa do sprostowania danych (art. 16),
- prawa do zapomnienia (art. 17),
- prawa do ograniczenia przetwarzania (art. 18),
- prawa do przenoszenia danych (art. 20),
- prawa do sprzeciwu (art. 21),
- prawa do niepodlegania automatycznym rozstrzygnięciom indywidualnym (art. 22).

Procedura realizacji żądań osób, których dane dotyczą

Każdy z administratorów danych z branży internetowej powinien opracować procedurę realizacji praw podmiotów danych, których dane przetwarza. Procedura powinna zawierać co najmniej takie elementy jak: zasady i tryb przyjmowania żądań (wniosków) podmiotów danych, termin i sposób ich rozpatrzenia, a także zasady postępowania w przypadku pozytywnego i negatywnego rozpoznania wniosku.

Procedurę realizacji praw podmiotów danych (użytkowników internetu) można opisać w pięciu, następujących krokach:

Po pierwsze, konieczne jest **przygotowanie procedury** wskazującej sposób realizacji żądań osób, których dane dotyczą oraz **udostępnienie adresu e-mail** bądź **formularza elektronicznego** do zgłaszania żądań.

Po drugie, niezbędne jest **ustalenie swojej roli,** tj. czy dla danych osobowych, których dotyczy żądanie, jest się administratorem (współadministratorem) tych danych czy też procesorem. Ma to istotne znaczenie prawne, adresatem obowiązków określonych w art. 12-22 RODO jest bowiem administrator danych. Jeżeli z analizy wynika, że podmiot, do którego skierowano wniosek, jest podmiotem przetwarzającym, niezbędne jest przekazanie tego żądania do właściwego administratora lub, jeżeli to przewiduje umowa z administratorem, rozpoznanie żądania zgodnie z instrukcjami administratora.

[35] IAB Europe GDPR Implementation Working Group Version 1.0 6 April 2018: *DATA SUBJECT REQUEST Working Paper 04/2018*.

Po trzecie, konieczne jest sprawdzenie, czy żądanie nie jest objęte **wyjątkiem od obowiązku realizacji żądania osoby**, których dane dotyczą (art. 11 ust. 1 RODO).

Po czwarte, **należy zweryfikować tożsamość osoby** występującej z żądaniem. Istotne jest, że w przypadku posiadania uzasadnionych wątpliwości co do tożsamości osoby występującej z żądaniem (użytkownika) podmiot z branży internetowej może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości takiej osoby (art. 12 ust. 6 RODO).

Po piąte, po dokonaniu wyżej wymienionych weryfikacji, podmiot z branży internetowej **realizuje żądanie** użytkownika bądź odmawia realizacji, jeżeli istnieją ku temu podstawy. Rozpatrzenie żądania następuje w terminie 30 dni od dnia otrzymania wniosku, co oznacza, że w tym terminie powinna zostać wysłana do wnioskodawcy informacja o sposobie rozpoznania wniosku. W razie potrzeby termin można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań (art. 12 ust. 3 RODO). W takim przypadku informację o przedłużeniu terminu należy przekazać w ciągu 30 dni od otrzymania żądania, powiadamiając o tym wnioskodawcę z podaniem przyczyn opóźnienia.

Administrator danych może zwrócić się do wnioskodawcy z wezwaniem o uzupełnienie wniosku, wraz z informacją, że jego nieuzupełnienie spowoduje odmowne rozpatrzenie wniosku, w sytuacjach gdy:

- podane we wniosku informacje nie umożliwiają przesłania odpowiedzi oraz kopii danych osobowych,
- wniosek jest niejasny lub niezrozumiały,
- wniosek dotyczy przekazania kopii danych lub przeniesienia danych, ale wnioskodawca nie określił zakresu danych do skopiowania lub przeniesienia,
- wniosek dotyczy przeniesienia danych, ale wnioskodawca zażądał użycia formatu danych lub technologii, które nie są stosowane przez danego administratora,
- wniosek dotyczy przeniesienia danych, ale wnioskodawca nie podał nazwy i adresu innego administratora lub podał błędny adres lub nazwę administratora, do którego zażądał przeniesienia danych.

W wezwaniu powinien zostać określony termin, w którym wnioskodawca powinien uzupełnić wniosek.

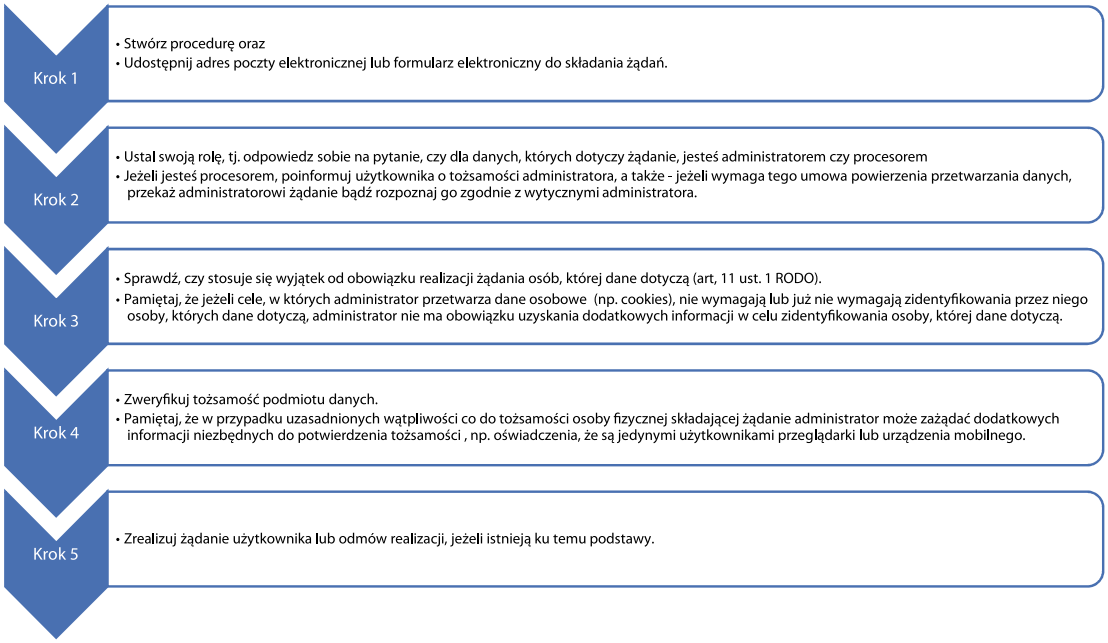
Administrator może negatywnie rozpatrzyć wniosek, w sytuacji gdy:

- wniosek jest nieuzasadniony, w szczególności gdy pozytywne załatwienie wniosku jest prawnie niedopuszczalne lub niewymagane,
- wniosek jest nadmiarowy, w szczególności gdy jest składany ustawicznie, co oznacza wniosek składany częściej niż raz na 2 miesiące w tej samej kategorii sprawy,
- brak możliwości technologicznych zrealizowania wniosku, np. w sytuacji wniosku o przeniesienie danych,
- wniosek nie został w terminie uzupełniony przez wnioskodawcę o informacje, pomimo wezwania wysłanego do wnioskodawcy.

W przypadku negatywnego rozpatrzenia wniosku skierowana do wnioskodawcy informacja powinna zawierać uzasadnienie negatywnej decyzji oraz pouczenie o możliwości wniesienia przez wnioskodawcę skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

W sytuacji pozytywnego rozpatrzenia wniosku podejmowane przez administratora działania powinny mieć na celu ochronię interesów podmiotów danych, np. w przypadku przekazywania kopii danych osobowych lub przeniesienia danych powinny być one dodatkowo zabezpieczane w zależności od formy ich przesyłania.

Poniżej przedstawiono schemat graficzny ww. procedury.



12. Schemat graficzny procedury realizacji praw podmiotów danych, których dane są przetwarzane

Problemy praktyczne z realizacją praw podmiotów danych w internecie

Największe problemy w branży internetowej z realizacją praw osób, których dane dotyczą, pojawiają się w przypadku realizacji żądań dotyczących udzielenia kopii danych i ich usunięcia. Większość tych podmiotów zbiera bowiem i przetwarza informacje, **które bezpośrednio nie identyfikują osób fizycznych** (tzw. dane pseudonimizowane), gdyż nie jest to ich celem. **Zaliczamy do nich pliki *cookie*, adres internetowy IP czy identyfikator telefonu komórkowego IMEI.** Pliki te identyfikują dane urządzenia i przeglądarki używane do przeglądania stron internetowych, nie dają jednak możliwości ustalenia tożsamości użytkownika, gdyż nie są w żaden sposób łączone z jego danymi osobowymi.

Administratorzy, będąc w posiadaniu wyłącznie tych danych, aby móc odpowiedzieć na żądanie, muszą wykonać dodatkowe działania, aby pozyskać dane umożliwiające identyfikację osoby. Zastosowanie w takim przypadku znajduje art. 11 ust. 1 RODO, który stanowi, **że administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą wyłącznie po to, aby zastosować się do wymogów określonych w RODO.** Zapis ten należy interpretować w ten sposób, że jeżeli administrator nie jest w stanie zidentyfikować osoby fizycznej na podstawie posiadanych danych osobowych, to ma on prawo – po uprzednim powiadomieniu tej osoby, o ile jest to możliwe,(art. 11 ust. 2 RODO) – odmówić realizacji praw wynikających z przepisów art. 15-20 RODO. Odmowa taka nie jest jednak dopuszczalna, jeżeli podmiot danych, na prośbę administratora, dostarczy dodatkowych informacji, które pozwolą na jego identyfikację.

W powyższym kontekście warto również przypomnieć, że podmiot z branży internetowej, jeżeli tylko ma uzasadnione wątpliwości w tym względzie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą (art. 12 ust. 6 RODO). W praktyce administratorzy z branży internetowej żądają od wnioskodawców np. złożenia oświadczenia, że są jedynymi posiadaczami czy użytkownikami przeglądarki lub urządzenia mobilnego, przy pomocy którego przetwarzane były dane osobowe objęte żądaniem.

W swoich wytycznych również Grupa Wdrożeniowa GDPR IAB Europe[36] zwraca szczególną uwagę na konieczność weryfikacji tożsamości osoby składającej wniosek z żądaniem realizacji praw. Jest to kluczowe w przypadku realizacji żądań dotyczących prawa do kopii danych, gdyż istnieje tu wysokie ryzyko naruszenia danych osobowych poprzez bezpodstawne udostepnienie osobom niepożądanym. Konsekwencje takiego działania przeważają nad potrzebą ujawnienia np. historii przeglądanych stron. Administratorzy z branży internetowej powinni więc stworzyć mechanizm do weryfikacji tożsamości, który pozwoli zidentyfikować użytkownika oraz spełnić żądania w zakresie zbierania jego aktywności na witrynach administratora. Sposoby weryfikacji powinny być szczegółowo opisane w procedurze realizacji praw podmiotów danych osobowych. Dotyczy to danych zarówno niepseudonimizowanych, takich jak adresy email, jak i pseudonimizowanych, takich jak identyfikatory internetowe (np. *cookies*).

a) Dane niepseudonimizowane

W przypadku danych niepseudonimizowanych, jeżeli użytkownik logował się do witryny poprzez formularz logowania, np. do poczty elektronicznej, forum czy sklepu internetowego, to wówczas wszystkie działania użytkownika przypisywane są do jego konta i administrator może je z łatwością uzyskać i udostępnić. W celu identyfikacji może poprosić o wypełnienie formularza na stronie firmy, kliknięcie w link weryfikacyjny czy podanie numeru PIN nadanego podczas rejestracji. W przypadku udostępniania danych wrażliwych wskazane jest stosowanie wieloetapowej weryfikacji. W przypadku gdyby użytkownik żądał podania mu wszystkich informacji, jakie zbiera wydawca za pomocą identyfikatorów, wówczas może on udostępnić jedynie informacje na temat stron aktywności, które zostały przypisane do zalogowanego konta użytkownika. Nie może podać danych o całej aktywności (zawartych w *cookies*), a które zostały zarejestrowane, gdyż istnieje możliwość, że aktywności na nich mogła dokonać inna osoba, gdy użytkownik nie był zalogowany i podanie tych informacji mogłoby negatywnie wpłynąć na prawa i wolności osoby, której dane dotyczą.

b) Dane pseudonimizowane

W przypadku posiadania wyłącznie danych pseudonimizowanych, jak identyfikatory internetowe, weryfikacja osoby, której dane dotyczą, wymaga zastosowania innych metod. Wynika to z faktu, iż z jednego urządzenia i jednej przeglądarki może korzystać kilka osób, np. w gospodarstwie domowym. Jeżeli nie logują się oni do konta w systemie komputera, ich czynności zostaną zarejestrowane pod jednym numerem *cookie*, zatem identyfikacja konkretnej osoby po stronie wydawców internetowych, bez dodatkowych informacji, jest niemożliwa. Grupa Wdrożeniowa w swoich wytycznych zwraca szczególną uwagę na to, iż administratorzy przetwarzający tego rodzaju dane powinni zażądać przesłania numeru identyfikatora, którego dotyczy żądanie, np. poprzez *screen* ekranu. Dodatkowo wskazuje się na możliwość zażądania złożenia deklaracji, a nawet oświadczenia pod rygorem prawnym, przez osobę wnoszącą żądanie, że jest ona właścicielem i operatorem przeglądarki lub urządzenia i ma prawo domagać się realizacji swoich praw na mocy art. 15-20 RODO[37].

[36] IAB Europe GDPR Implementation Working Group Version 1.0 6 April 2018: *DATA SUBJECT REQUEST Working Paper 04/2018, s. 8-9*.

[37] IAB Europe GDPR Implementation Working Group Version 1.0 6 April 2018: *DATA SUBJECT REQUEST Working Paper 04/2018, s. 10*.

Podsumowując, ze względu na trudność identyfikacji osoby fizycznej wyłącznie na podstawie identyfikatorów *cookie*, IP czy IMEI oraz w związku z ryzykiem ujawnienia informacji nieupoważnionym podmiotom, Grupa Wdrożeniowa, przed udzieleniem odpowiedzi na żądanie, zaleca rozważenie zastosowania jednej z poniższych możliwości:

- jasne i czytelne określenie w procedurze realizacji praw, czy administrator ma możliwość identyfikowania osób składających żądanie i czy będzie odpowiadać na wnioski dotyczące identyfikatorów,
- jasne i czytelne określenie w procedurze realizacji praw, w jaki sposób realizowane są żądania podmiotów oraz jakie informacje są niezbędne do identyfikacji osoby i przyjęcia wniosku z żądaniem dotyczącym identyfikatorów (w tym oświadczenia i skany z ekranu),
- utworzenie strony internetowej, która umożliwi administratorowi sprawdzenie plików *cookie* osoby składającej żądanie na określonej przeglądarce.[38]

[38] Ibid., s. 11.

SŁOWNICZEK RODO

A

Administrator danych – podmiot decydujący o celach i sposobach przetwarzania danych osobowych. Administrator danych jest adresatem wszystkich obowiązków określonych w RODO. W przypadku gdy decyzje podejmowane są wspólnie przed kilka podmiotów, są one współadministratorami.

C

Consent Management Platform (CMP) – oprogramowanie umożliwiające operatorom stron internetowych uzyskiwanie zgody na przetwarzanie danych osobowych użytkowników internetu, przechowywanie informacji o uzyskanych zgodach oraz przesyłanie informacji o zgodzie udzielonej przez określonego użytkownika do innych uczestników rynku RTB (SSP, DSP, DMP).

D

Dane pseudonimizowane – dane przetworzone w taki sposób, aby nie można było ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, np. identyfikator IP, plik *cookie*.

Data Management Platform (DMP) – platforma zarządzania danymi, udostępniająca dane o użytkownikach (lub segmenty tych danych, opracowane w oparciu o kryteria behawioralne lub demograficzne) i umożliwiająca wykorzystywanie przez reklamodawców danych z różnych źródeł w celu optymalizacji kampanii reklamowych.

Demand Side Platform (DSP) – platforma popytowa umożliwiająca reklamodawcom zarządzanie procesem zakupu powierzchni reklamowej bezpośrednio od wydawców lub od platform SSP.

G

Grupa Robocza Art. 29 – organ o charakterze doradczym, powołany na mocy art. 29 dyrektywy 95/46/WE, w skład którego wchodzili m.in. przedstawiciele organu lub organów nadzorczych z państw członkowskich UE. Do zadań Grupy należało m.in. przyczynianie się do jednolitego stosowania przepisów o ochronie danych w państwach UE. Grupa ta została rozwiązana 25 maja 2018 roku, a w jej miejsce została powołana Europejska Rada Ochrony Danych.

I

IAB Europe – europejskie stowarzyszenie branży reklamy internetowej z siedzibą w Brukseli skupiające firmy i organizacje krajowe cyfrowego ekosystemu reklamowego. Jego misją jest promowanie rozwoju tego innowacyjnego sektora poprzez kształtowanie otoczenia regulacyjnego, promowanie wartości, jakie reklama cyfrowa wnosi do gospodarki Unii Europejskiej, a także korzyści dla konsumentów. Organizacja rozwija i ułatwia wdrażanie zharmonizowanych praktyk biznesowych.

IAB Polska – Związek Pracodawców Branży Internetowej IAB Polska, organizacja zrzeszająca ok. 230 firm członkowskich z branży internetowej, w tym portale internetowe, sieci reklamowe, domy mediowe, agencje interaktywne i reklamodawców. Misją IAB jest wspieranie działalności uczestników rynku komunikacji interaktywnej oraz popularyzacja internetu jako efektywnego medium poprzez działania promocyjne, badawcze, edukacyjne oraz *public affairs*.

M

Model tradycyjny reklamy internetowej – w przeciwieństwie do modelu reklamy typu *programmatic* udzielenie zlecenia nie odbywa się za pomocą platformy informatycznej, lecz bezpośrednio poprzez działy handlowe poszczególnych podmiotów zaangażowanych w proces.

O

Obowiązek informacyjny – obowiązek administratora podania podmiotowi danych informacji określonych w RODO. Obowiązek ten aktualizuje się na etapie zbierania danych osobowych. Powinien być wykonywany z inicjatywy administratora danych, tj. bez konieczności występowania z dodatkowym żądaniem przez podmiot danych.

OpenRTB – protokół określający zasady komunikacji pomiędzy uczestnikami aukcji RTB (w szczególności – platformami DSP i SSP), w tym obligatoryjne, rekomendowane i opcjonalne kategorie danych udostępniane w ramach aukcji.

P

Podmiot przetwarzający dane (procesor) – podmiot dokonujący przetwarzania danych osobowych w imieniu administratora. Jest nim często zleceniobiorca usług reklamowych. Podmiot ten powinien dawać gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, nie odpowiada natomiast za inne obowiązki, których adresatem jest administrator danych (np. obowiązek informacyjny, obowiązek określenia podstawy prawnej przetwarzania).

Prawo dostępu do danych osobowych – prawo podmiotu danych do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce – do uzyskania informacji o przetwarzaniu oraz kopii danych osobowych.

Prawo do bycia zapomnianym – prawo podmiotu danych do żądania od administratora danych usunięcia danych osobowych. Prawo to nie jest bezwzględne i w sytuacjach określonych w RODO administrator danych może odmówić jego realizacji.

Prawo do przenoszenia danych – prawo podmiotu danych do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz prawo przesłania tych danych osobowych innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Prawo do przenoszenia danych nie jest bezwzględne i w sytuacjach określonych w RODO administrator danych może odmówić jego realizacji.

Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Należy rozróżnić profilowanie „zwykłe", wykonywane na potrzeby marketingu bezpośredniego (art. 21 ust. 2-3 RODO) oraz profilowanie „kwalifikowane", wykonywane na potrzeby „zautomatyzowanych decyzji", a więc decyzji podejmowanych bez udziału człowieka i mających istotne skutki prawne dla podmiotów danych (art. 22 RODO). W przypadku przetwarzania danych osobowych na potrzeby reklamy internetowej mamy jednak przeważnie do czynienia z profilowaniem „zwykłym", jego wykonywanie jest dopuszczalne do czasu wyrażenia przez tę osobę sprzeciwu (art. 21 ust. 3 RODO).

Programmatic Media Buying – model nabywania powierzchni reklamowej dostępnej na stronach internetowych lub w aplikacjach mobilnych w sposób zautomatyzowany, przy użyciu dedykowanego oprogramowania i algorytmów.

PT – Prawo Telekomunikacyjne, ustawa z dnia 16 lipca 2004 r. (tekst jednolity Dz. U. z 2018 r., poz. 1954). Przepisy PT określają zasady dopuszczalnego korzystania z *cookies* (art.173).

PUODO – Prezes Urzędu Ochrony Danych Osobowych.

R

Retargeting – rodzaj internetowych kampanii reklamowych polegających na adresowaniu spersonalizowanych komunikatów reklamowych do użytkowników, którzy mieli już kontakt z produktami reklamodawcy, np. poprzez wizytę na jego stronie internetowej.

RODO – 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. Rozporządzenie obowiązuje od 25 maja 2018 r.

RTB (Real-Time Bidding) – model nabywania poszczególnych wyświetleń reklam na powierzchniach reklamowych dostępnych na stronach internetowych lub w aplikacjach mobilnych w trybie aukcji prowadzonych na podstawie zestandaryzowanych protokołów w czasie rzeczywistym.

S

Supply Side Platform (SSP) – platforma podażowa oferująca powierzchnie reklamowe dostępne na stronach wydawców platformom DSP, bezpośrednio lub poprzez tzw. giełdy reklam (*ad exchanges*).

T

Test równowagi – dotyczy sytuacji powołania się na przesłankę prawnie uzasadnionego interesu (art. 6 ust. 1 pkt f RODO), *opt-out*. W takim przypadku administrator ma obowiązek przeprowadzić ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu i na podstawie tego testu zdecydować, czy interes ten jest uzasadniony. W wyniku analizy administrator powinien określić, czyje interesy – jego własne czy osoby, której dane dotyczą – są w danych okolicznościach przeważające. W przypadku gdy będzie nim interes podmiotu danych, przetwarzanie jest niedopuszczalne.

Tradycyjna reklama internetowa – patrz: Model tradycyjny reklamy internetowej.

Transparency & Consent Framework (TCF) – Ramy Przejrzystości i Zgody – mechanizm zaprojektowany przez IAB Tech Lab oraz IAB Europe mający na celu wsparcie branży internetowej, a w szczególności wydawców, dostawców usług technologicznych, agencji interaktywnych i reklamodawców w wypełnianiu obowiązków z przepisów rozporządzenia (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych i swobodnego przepływu tych danych (RODO) dotyczących podstaw prawnych przetwarzania danych osobowych użytkownika (w szczególności przepisy dotyczące zgody i uzasadnionego interesu). Więcej informacji: https://advertisingconsent.eu/

TSUE – Trybunał Sprawiedliwości Unii Europejskiej.

U

UODO – Urząd Ochrony Danych Osobowych.

Ustawa o ochronie danych osobowych – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000), uzupełniająca przepisy RODO. Ustawa weszła w życie w dniu 25 maja 2018 r.

Uśude – ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jednolity – Dz.U. z 2019 r., poz. 123). W zakresie przepisów o ochronie danych osobowych w związku ze świadczeniem usług drogą elektroniczną ustawa uzupełnia RODO.

AUTORZY

Wszyscy autorzy raportu są ekspertami Zespołu RODO IAB Polska.

Jakub Borkowski

Inspektor ochrony danych w Adrino sp. z o. o., Netsprint S.A. oraz Leadr sp. z o. o. Web developer z ponad 10-letnim doświadczeniem, związany z branżą reklamy internetowej od 5 lat. Specjalizujący się w szeroko pojętym bezpieczeństwie danych, w szczególności ochronie danych osobowych oraz wykrywaniu nadużyć w reklamie internetowej (ang. *ad fraud*).

Magdalena Kogut-Czarkowska

Specjalizuje się w ochronie danych osobowych i prawie własności intelektualnej, ze szczególnym uwzględnieniem kwestii handlu elektronicznego i ochrony konsumentów. Doradza klientom w zakresie przestrzegania przepisów o ochronie prywatności, w szczególności w odniesieniu do umów dotyczących przetwarzania danych, korzystania z baz danych w ramach grup kapitałowych, outsourcingu przetwarzania danych, transgranicznych przepływów danych, naruszeń prywatności oraz sprzedaży, dzierżawy i rejestracji baz danych. Doradza spółkom działającym w branży informatycznej w zakresie wdrażania systemów komputerowych, w tym udzielania licencji. Zajmuje się również sporami dotyczącymi własności intelektualnej. Uzyskała rekomendację Legal 500 EMEA jako Prawnik Nowego Pokolenia w 2018 oraz 2019 roku. Jest członkiem grup roboczych IAB Prawnej i RODO. Magdalena została również powołana przez Ministerstwo Cyfryzacji w Polsce do Grupy Roboczej do spraw Internetu Rzeczy.

Xawery Konarski

Adwokat, starszy partner. Ekspert prawny z ponad 20-letnim doświadczeniem w nowych technologiach. Starszy partner i współzałożyciel kancelarii Traple Konarski Podrecki i Wspólnicy. W kancelarii nadzoruje prace zespołów: Technologie, Media, Telekomunikacja (TMT). Doradza polskim i międzynarodowym przedsiębiorstwom w zakresie prawa telekomunikacyjnego, IT, internetu oraz ochrony danych osobowych. Zasiada w Radzie Polskiej Izby Informatyki i Telekomunikacji (PIIT), jest członkiem zarządu PIIT. Jest doradcą prawnym Związku Pracodawców Branży Internetowej IAB Polska oraz Polskiej Izby Ubezpieczeń (PIU). Jako ekspert brał udział w pracach legislacyjnych nad szeregiem ustaw z zakresu prawa nowych technologii, w tym ustawy o ochronie danych osobowych. Jest arbitrem Sądu Polubownego ds. domen internetowych przy PIIT. Doradza izbom gospodarczym oraz związkom pracodawców przy tworzeniu kodeksów postępowania dotyczących wdrożenia RODO. Wielokrotnie rekomendowany w polskich i zagranicznych rankingach prawników specjalizujących się w TMT (m.in. Chambers Europe, Legal 500, Rzeczpospolita). Autor kilkudziesięciu pozycji naukowych z zakresu prawa nowych technologii i ochrony danych osobowych, w tym komentarza do ustawy o świadczeniu usług drogą elektroniczną.

Katarzyna Ksionek

Starszy prawnik, specjalizuje się w prawie handlowym, zagadnieniach dotyczących ochrony danych osobowych, IT, IPR, prawnych aspektach działalności mediów, reklamy i e-commerce, doradza przy projektach finansowych, reorganizacyjnych i transakcjach M&A w grupie kapitałowej Wirtualna Polska Holding S.A.

Ewa Nitkiewicz

Starszy prawnik specjalista w Grupie RAS Polska, koordynowała prace RODO Team w Grupie RAS Polska, Fundacji Faktu, City-Nav. Specjalizuje się w prawie ochrony danych osobowych, IT, IPR, mediów i reklamy. Doktorant UJ. Studia i stypendia: Paris X Nanterre, Europa Kolleg & Hamburg Universitaet. Pracowała w firmach IT (m.in. Comarch S.A.), w Roedl Korpalski Kancelaria Prawna sp. k., w Międzynarodowej Organizacji IOM w Genewie.

Wojciech Piszewski

Autor jest adwokatem, współpracującym ze spółką Agora S.A., w której pełni m.in. funkcję compliance officera. Obok dotychczasowych działań związanych z obsługą klientów na gruncie korporacyjnym i procesowym, aktualnie specjalizuje się również w zakresie prawa własności intelektualnej i prawa ochrony danych osobowych. Szeroko wspierał spółki z grupy kapitałowej Agora w procesie wdrożenia wymagań RODO.

Żaneta Sadowska

Od czasu wejścia w życie RODO pełni funkcję inspektora ochrony danych w spółkach Time S.A., ZPR Media S.A., IDM Net S.A., Afilo sp. z o. o. Z branżą internetową związana jest od 2006 roku. Przez 7 lat zajmowała się sprzedażą powierzchni reklamowych oraz promocją m.in. dla portalu Gazeta.pl. Z Grupą ZPR Media związana jest od 5 lat, gdzie rozwijała swoje kompetencje jako product i project manager, budując dział wsparcia reklamy internetowej dla radiowego pionu sprzedaży regionalnej. Jednocześnie zdobywała i poszerzała swoją wiedzę na temat ochrony danych osobowych, uczestnicząc w wielu konferencjach, kongresach i szkoleniach. Ukończyła studia podyplomowe w INP PAN o kierunku Wykonywanie funkcji inspektora ochrony danych.

Przemysław Szymański

LL. M., Head of Legal & Compliance, RTB House SA, radca prawny specjalizujący się w zagadnieniach dotyczących ochrony danych osobowych, prawa nowych technologii oraz prawa kontraktów handlowych. Doświadczenie zawodowe zdobywał w międzynarodowych i polskich kancelariach prawnych. Absolwent wydziałów prawa Uniwersytetu Warszawskiego oraz University of Edinburgh (LL.M. in Commercial Law).

Magdalena Tomaszewska

Jest radcą prawnym, inspektorem ochrony danych w Grupie naTemat. Jest absolwentką Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego. Ukończyła także Prawo Nowych Technologii na Akademii Leona Koźmińskiego oraz Prawo Francuskie i Europejskie na Uniwersytecie Warszawskim w partnerstwie z Uniwersytetem w Poitiers. Doświadczenie zdobyła w administracji państwowej oraz w kancelariach międzynarodowych i krajowych. Autorka publikacji naukowych. Specjalizuje się w zagadnieniach związanych z prawem konkurencji, prawem nowych technologii i prawem ochrony danych osobowych. Wdrażała RODO w wielu spółkach prawa handlowego.

Jan Tyski

Jest radcą prawnym, pełni funkcję inspektora ochrony danych m.in. w Tarsago Polska sp. z o. o. Zawodowo związany z prawem ochrony danych osobowych i prawem nowych technologii. Wspierał spółki z Tarsago Media Group we wdrożeniu RODO. Wcześniej pracował w Biurze GIODO, a także w firmie konsultingowej, gdzie szkolił i doradzał klientom w obszarze ochrony danych osobowych.

iab polska

RODO

Redakcja merytoryczna
mec. Xawery Konarski

Redakcja i korekta
Ewa Ziętek-Maciejczyk

Projekt graficzny i skład
Krzysztof Kowalczyk

Koordynacja projektu
Anna Mazur

Związek Pracodawców Branży Internetowej IAB Polska

tel.: 22 415 54 44

biuro@iab.org.pl

www.iab.org.pl