enterprise
europe
network

POLSKA

BIULETYN EURO INFO

2 (205) 2021
www.een.org.pl

Artykuły zgodne
ze standardem WCAG 2.0
na www.een.org.pl

WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

NOWA USTAWA – PRAWO KOMUNIKACJI ELEKTRONICZNEJ

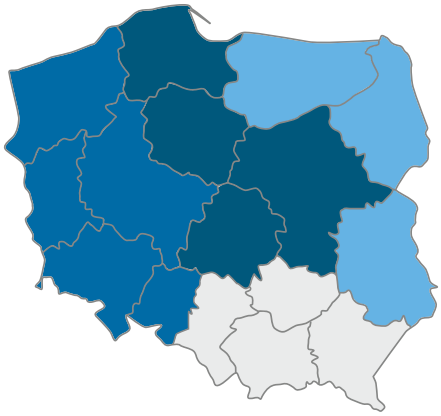
ŚWIADCZENIE PRACY ZDALNEJ PRZEZ CUDZOZIEMCA

ISSN 2544-4719

PARP Grupa PFR Centrum Rozwoju MŚP

enterprise europe network
Wsparcie dla biznesu w zasięgu ręki

Konsorcja realizujące projekt Enterprise Europe Network w Polsce



Enterprise Europe Network – Central Poland

Enterprise Europe Network – East Poland

Enterprise Europe Network – West Poland

Enterprise Europe Network – South Poland

Konsorcjum: Enterprise Europe Network-Central Poland

Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83, 00-834 Warszawa
tel. (22) 432 71 02
www.een.org.pl

Instytut Mechanizacji Budownictwa i Górnictwa Skalnego
ul. Racjonalizacji 6/8, 02-673 Warszawa
tel. (22) 847 53 68
www.een-centralpoland.eu

Fundacja Rozwoju Przedsiębiorczości
ul. Piotrkowska 86, 90-103 Łódź
tel. (42) 630 36 67
www.frp.lodz.pl

Stowarzyszenie „Wolna Przedsiębiorczość"
ul. Piekarnicza 12A
80-126 Gdańsk
tel. 58 350 51 40
www.een.pomorskie.pl

Toruńska Agencja Rozwoju Regionalnego SA
ul. Włocławska 167, 87-100 Toruń
tel. (56) 699 54 80-83
www.een.tarr.org.pl

Uniwersytet Warszawski DELab
ul. Dobra 56/66, 00-312 Warszawa
tel. (22) 55 27 606
www.delab.uw.edu.pl/pl/een/

Konsorcjum: Enterprise Europe Network-East Poland

Podlaska Fundacja Rozwoju Regionalnego
ul. Starobojarska 15, 15-073 Białystok
tel. (85) 740 86 83
www.pfrr.pl, www.een-polskawschodnia.pl,
www.een.pfrr.pl

Centrum Innowacji i Transferu Technologii, Uniwersytet Warmińsko-Mazurski w Olsztynie
ul. Prawocheńskiego 9, 10-720 Olsztyn
tel. (89) 523 39 00
www.uwm.edu.pl, www.een-polskawschodnia.pl,
www.uwm.edu.pl/een

Warmińsko-Mazurska Agencja Rozwoju Regionalnego SA w Olsztynie
ul. Jagiellońska 91a, 10-356 Olsztyn
tel. (89) 512 24 05
www.een.wmarr.olsztyn.pl,
www.een-polskawschodnia.pl

Centrum Innowacji i Transferu Technologii Politechniki Lubelskiej
ul. Nadbystrzycka 38H, 20-618 Lublin
tel. (81) 538 42 70
http://lctt.pollub.pl,
www.een-polskawschodnia.pl,
www.citt.pollub.pl

Lubelska Fundacja Rozwoju
Rynek 7, 20-111 Lublin
tel. (81) 528 53 11-12-31
www.lfr.lublin.pl,
www.een-polskawschodnia.pl

Park Naukowo-Technologiczny Polska Wschód w Suwałkach Sp. z o.o.
ul. Innowacyjna 1, 16-400 Suwałki
tel. (87) 564 22 24-25
www.park.suwalki.pl,
www.een-polskawschodnia.pl

Konsorcjum: Enterprise Europe Network-South Poland

Centrum Transferu Technologii, Politechnika Krakowska
ul. Warszawska 24, 31-155 Kraków
tel. (12) 628 28 45
www.transfer.edu.pl

Izba Przemysłowo-Handlowa w Krakowie
ul. Floriańska 3, 31-019 Kraków
(12) 428 92 55
www.iph.krakow.pl

Górnośląska Agencja Przedsiębiorczości i Rozwoju sp. z o.o.
ul. Wincentego Pola 16, 44-100 Gliwice
tel. (32) 339 31 10
www.gapr.pl

Fundusz Górnośląski SA Oddział w Katowicach
ul. Powstańców 17, 40-039 Katowice
tel. 32 72 85 828
www.enterprise.fgsa.pl

Świętokrzyskie Centrum Innowacji i Transferu Technologii Sp. z o.o.
ul. Studencka 1, 25-323 Kielce
tel. (41) 343 29 10
www.it.kielce.pl

Staropolska Izba Przemysłowo-Handlowa
ul. Sienkiewicza 53, 25-002 Kielce
tel. (41) 368 02 78
www.siph.com.pl

Rzeszowska Agencja Rozwoju Regionalnego SA
ul. Szopena 51, 35-959 Rzeszów
tel. (17) 867 62 34
www.rarr.rzeszow.pl

Stowarzyszenie Grupy Przedsiębiorców Przemysłu Lotniczego Dolina Lotnicza
ul. Szopena 51, 35-959 Rzeszów
tel. (17) 850 19 35
www.dolinalotnicza.pl

Wyższa Szkoła Informatyki i Zarządzania
ul. mjr. H. Sucharskiego 2, 35-225 Rzeszów
tel. (17) 852 49 75
www.een.wsiz.pl

Konsorcjum: Enterprise Europe Network-West Poland

Wrocławskie Centrum Transferu Technologii, Politechnika Wrocławska
ul. Smoluchowskiego 48, 50-372 Wrocław
tel. (71) 320 33 18
www.wctt.pwr.edu.pl

Poznański Park Naukowo-Technologiczny Fundacji Uniwersytetu im. Adama Mickiewicza
ul. Rubież 46, 61-612 Poznań
tel. (+48) 61 827 97 46
www.ppnt.poznan.pl

Agencja Rozwoju Regionalnego SA w Koninie
ul. Zakładowa 4, 62-510 Konin
tel. (+48) 63 245 30 95
www.arrkonin.org.pl

Centrum Przedsiębiorczości i Transferu Technologii Uniwersytetu Zielonogórskiego
ul. Syrkiewicza 6, 66-002 Nowy Kisielin
tel. (+48) 504 070 281
www.cptt.uz.zgora.pl

Fundacja Kaliski Inkubator Przedsiębiorczości
ul. Częstochowska 25, 62-800 Kalisz
tel. (+48) 62 765 60 58
www.kip.kalisz.pl

Dolnośląska Agencja Rozwoju Regionalnego SA
ul. Szczawieńska 2, 58-310 Szczawno-Zdrój
tel. (+48) 74 648 04 50
www.darr.pl

Stowarzyszenie „Promocja Przedsiębiorczości" w Opolu
ul. Damrota 4, 45-064 Opole
tel. (+48) 77 456 56 00
www.een.opole.pl

Regionalne Centrum Innowacji i Transferu Technologii
ul. Jagiellońska 20-21, 70-363 Szczecin
tel. (+48) 91 449 41 09
www.innowacje.zut.edu.pl

Zachodniopomorskie Stowarzyszenie Rozwoju Gospodarczego – Szczecińskie Centrum Przedsiębiorczości
ul. Kolumba 86, 70-035 Szczecin
tel. (+48) 91 433 02 20
www.zsrg.szczecin.pl/een/

Drodzy Czytelnicy,

Rozporządzenie Ogólne o Ochronie Danych, czyli RODO, przewidziało w swoich przepisach instytucję współadministrowania danymi osobowymi. Nie jest to zupełnie nowe rozwiązanie. Przed wejściem w życie Rozporządzenia taki sposób decydowania o celach i sposobach przetwarzania danych osobowych jak najbardziej występował, a wraz ze wzrostem znaczenia danych dla światowej gospodarki zyskiwał na znaczeniu. Dodatkowo w ostatnim czasie współadministrowanie zostało wzmocnione przez orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (np. tzw. sprawa Fashion ID). I bez większego ryzyka można stwierdzić, że w przyszłości będzie występowało coraz częściej, chociażby z racji wspólnych działań podejmowanych przez różne podmioty w walce z pandemią koronawirusa. Czym jednak jest współadministrowanie i w jakich sytuacjach do niego dochodzi? Na to pytanie poszukujemy odpowiedzi w artykule pt. „Współadministrowanie danymi osobowymi. Kwalifikacja, obowiązki i zakres odpowiedzialności".

Polecamy także artykuł dotyczący projektu nowej ustawy – Prawo komunikacji elektronicznej. Z jego treści dowiemy się, jakie zmiany w tym obszarze wprowadzi polski ustawodawca w związku z implementacją do krajowego porządku prawnego przepisów unijnej dyrektywy.

Zapraszamy także do zapoznania się z najnowszymi ofertami współpracy zagranicznej pochodzącymi z bazy POD (*Partnership Opportunities Database*), prowadzonej przez Komisję Europejską i udostępnianej ośrodkom Enterprise Europe Network.

Z wyrazami szacunku
zespół redakcyjny
Biuletynu Euro Info

Spis treści

4 | Ochrona danych osobowych
Współadministrowanie danymi osobowymi

8 | Ochrona danych osobowych
Polityka prywatności na stronach internetowych

12 | Innowacje
Otwarte dane filarem innowacyjnej gospodarki

17 | Komunikacja elektroniczna
Nowa ustawa – Prawo komunikacji elektronicznej

21 | Marketing
Marketing e-mailowy

26 | Prawo pracy
Świadczenie pracy zdalnej przez cudzoziemca

31 | Oferty współpracy

Biuletyn Euro Info, wydawany przez ośrodek Enterprise Europe Network przy Polskiej Agencji Rozwoju Przedsiębiorczości, jest współfinansowany przez Komisję Europejską ze środków pochodzących z programu COSME na lata 2014–2020 oraz przez Ministerstwo Rozwoju, Pracy i Technologii w ramach programu pn. „Udział Polski w programie na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz w instrumentach finansowych programów UE wspierających konkurencyjność przedsiębiorstw w latach 2015–2021".

Redaktor naczelny: Paweł Sikorski
Zespół: Aleksandra Wolska, Agata Kudelska, Eryk Rutkowski
Korekta: Pracownia C&C Sp. z o.o.
Adres redakcji: Enterprise Europe Network przy PARP
ul. Pańska 81/83, 00-834 Warszawa
Telefon: 22 432 71 02

Skład, druk i dystrybucja: Pracownia C&C Sp. z o.o.
www.ccpg.com.pl
Zdjęcia: AdobeStock
Nakład: 1400 egz.

Współadministrowanie danymi osobowymi

Kwalifikacja, obowiązki oraz zakres odpowiedzialności

Bartosz Jussak

Przy współpracy kilku podmiotów, w ramach której dochodzi do przetwarzania danych osobowych, podmioty te mogą posiadać różny status w rozumieniu przepisów z zakresu ochrony danych osobowych. Właściwe zakwalifikowanie roli danego podmiotu w ramach konkretnych czynności przetwarzania danych osobowych ma duże znaczenie w szczególności dla określenia zarówno ciążących na nim obowiązków, jak i zakresu odpowiedzialności. Jednym z typów podmiotów, wskazanych w przepisach z zakresu ochrony danych osobowych, są współadministratorzy. Instytucja współadministrowania, chociaż nie nowa, dopiero w ostatnich latach zyskuje praktycznie znaczenie, w szczególności w związku z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej, w którym widać tendencję do rozszerzania stosowania tej instytucji. Warto zatem przyjrzeć się jej bliżej.

Współadministrator, administrator, podmiot przetwarzający

Zgodnie z art. 26 ust. 1 zd. 1 RODO, jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. Aby zatem mówić o współadministrowaniu, muszą być spełnione dwa warunki:

1. w relacji pozostaje co najmniej dwóch administratorów oraz
2. wspólnie ustalają oni cele i sposoby przetwarzania danych osobowych.

Możliwość wspólnego ustalania celów i sposobów przetwarzania wynika jednocześnie z samej definicji administratora zawartej w art. 4 pkt 7 RODO, gdzie wyraźnie wskazano, że administrator może ustalać cele i sposoby przetwarzania samodzielnie lub wspólnie z innymi.

W celu spełnienia pierwszego ze wspomnianych warunków, należy ocenić, czy każdy z podmiotów pozostających w danej relacji może być uznany za administratora w rozumieniu art. 4 pkt 7 RODO. Pozwoli to odróżnić relacje pomiędzy administratorami od relacji pomiędzy administratorami a podmiotami przetwarzającymi.

Relacja administrator – podmiot przetwarzający

Do rozróżnienia administratora i podmiotu przetwarzającego kluczowe znaczenie ma określenie, kto w ramach konkretnych czynności przetwarzania danych osobowych ustala cele i sposoby tego przetwarzania. Administrator jest podmiotem, który decyduje o pewnych kluczowych elementach dotyczących przetwarzania. Pomocne dla analizy może być w tym zakresie udzielenie odpowiedzi na pytania: kto decyduje o tym, że przetwarzanie danych ma miejsce oraz o tym, że przetwarzanie danych powinno nastąpić w określonym celu, a także kto odnosi korzyści z przetwarzania. Jednocześnie warto wskazać, że pojęcie administratora jest pojęciem funkcjonalnym, zatem analiza powinna opierać się na ocenie okoliczności faktycznych określonych czynności przetwarzania, a w mniejszym stopniu na analizie formalnej danej relacji.
Status administratora może wynikać z treści przepisów prawa (pośrednio lub bezpośrednio) i analizy okoliczności faktycznych danego przypadku (konkretnych działań poszczególnych podmiotów w określonym kontekście).
Określanie celów przetwarzania można sprowadzić do odpowiedzi na pytanie: **dlaczego dane są przetwarzane**. Innymi słowy chodzi tutaj o określanie, jaka wartość ma zostać osiągnięta w wyniku przetwarzania danych. Z kolei określanie sposobów przetwarzania można sprowadzić do pytania: **jak ww. cele przetwarzania mają być osiągnięte (jakimi środkami)**.

Jak wskazano wyżej, administrator musi decydować o obu tych elementach. W wytycznych właściwych organów oraz orzecznictwie rozróżnia się jednak kluczowe (zasadnicze) sposoby przetwarzania oraz pozostałe (niekluczowe) sposoby przetwarzania. Podział ten pomaga przeanalizować, jaki zakres autonomii w decydowaniu o sposobach przetwarzania danych może posiadać podmiot przetwarzający.

Podmiot przetwarzający, zgodnie z definicją zawartą w art. 4 pkt 8 RODO, jest podmiotem, który przetwarza dane osobowe w imieniu administratora. Przetwarzanie powierzonych podmiotowi przetwarzającemu danych odbywa się więc w celach określonych przez administratora i tylko administrator może je ustalać. Jeśli chodzi natomiast o sposoby przetwarzania, jak wskazano wyżej, administrator musi ustalać przynajmniej kluczowe sposoby przetwarzania.

Należy tutaj wskazać w szczególności na określanie tego: jakie dane (rodzaje danych) mają być przetwarzane, jak długo dane powinny być przetwarzane, kto może uzyskiwać dostęp do przetwarzanych danych (kto może być ich odbiorcą), dane jakich kategorii osób są przetwarzane itd. Podejmowanie decyzji w stosunku do innych niż kluczowe sposobów przetwarzania można często przekazać podmiotom przetwarzającym. Chodzi tutaj m.in. o decyzje dotyczące kwestii technicznych i organizacyjnych, np. decydowanie przez podmiot przetwarzający jako usługodawcy o tym, jaki typ oprogramowania jest wykorzystywany oraz o szczegółach dotyczących środków mających zapewnić bezpieczeństwo przetwarzania danych osobowych w takim zakresie, w jakim dokonuje tego podmiot przetwarzający.

Na marginesie należy również wskazać, że dla posiadania statusu administratora w stosunku do określonych danych, nie jest konieczne posiadanie faktycznego do nich dostępu. Kluczowe znaczenie ma tutaj sprawowanie faktycznej kontroli nad przetwarzaniem danych osobowych. Faktyczne przetwarzanie danych osobowych może zostać powierzone podmiotowi przetwarzającemu. Podsumowując ten fragment artykułu, można wskazać, że dla posiadania statusu administratora niezbędne jest decydowanie o celach oraz o kluczowych sposobach przetwarzania danych osobowych.

Relacje pomiędzy administratorami

Potwierdzenie, że w ramach danej relacji nie występuje stosunek powierzenia przetwarzania danych, a w konsekwencji, że w ramach danej relacji występują tylko administratorzy danych pozwala na przeprowadzenie dalszej analizy w celu oceny, czy w ramach współpracy występują współadministratorzy, czy osobni (samodzielni) administratorzy.

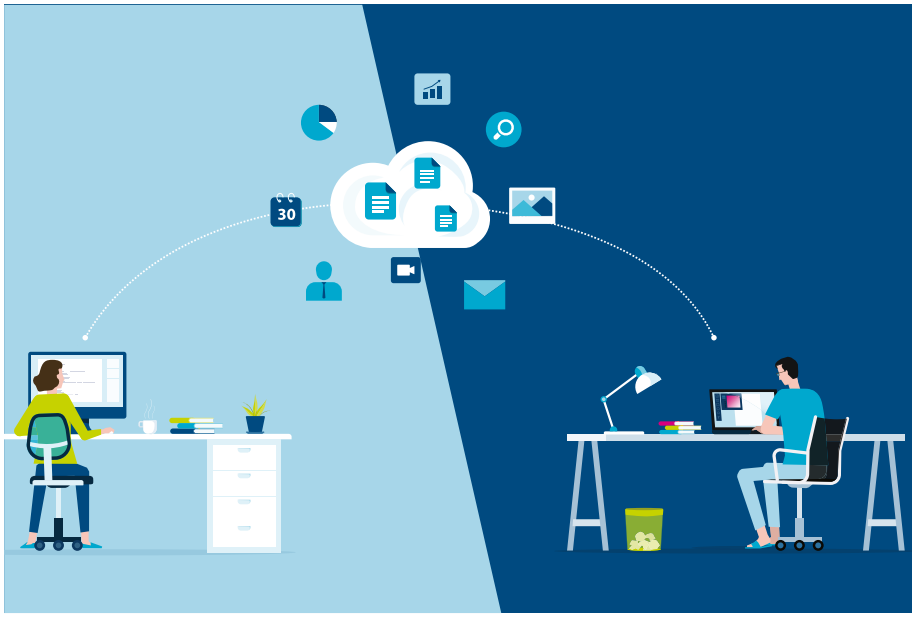
Dla stwierdzenia, że pomiędzy administratorami dochodzi do współadministrowania danymi osobowymi, niezbędne jest to, żeby **wspólnie** ustalali oni cele i sposoby przetwarzania danych. Jeśli bowiem w danej relacji występują wprawdzie tylko administratorzy, ale każdy z nich samodzielnie ustala cele i sposoby przetwarzania danych, nie będzie dochodziło do współadministrowania i będziemy mieli do czynienia z relacją niezależnych administratorów. Należy również od razu wskazać, że mogą oczywiście wystąpić sytuacje, w których w pewnym zakresie współpracujące podmioty będą posiadały status współadministratorów, a w pewnym zakresie niezależnych administratorów.

Wspólny udział w ustalaniu celów i sposobów przetwarzania może przybrać przy tym różne formy. Najbardziej intuicyjna wydaje się forma, w której podmioty wspólnie podejmują określone decyzje. Jednak na podstawie orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE) wyróżnia się również wspólny udział w ustalaniu celów i sposobów przetwarzania na podstawie „zbieżnych decyzji" poszczególnych podmiotów. Decyzje można uznać za zbieżne w zakresie celów i sposobów przetwarzania, jeśli się uzupełniają i są niezbędne do tego, aby przetwarzanie miało miejsce, poprzez wymierny wpływ na określenie celów i sposobów przetwarzania. Ważnym kryterium identyfikacji zbieżnych decyzji w tym kontekście jest określenie, czy przetwarzanie nie byłoby możliwe bez udziału obu stron, tzn. że przetwarzanie przez każdą ze stron jest nierozerwalnie połączone. Ze względu na nieostre kryteria uznanie, że podmioty wspólnie uczestniczą w ustalaniu celów i sposobów przetwarzania w formie „zbieżnych decyzji", może rodzić w praktyce duże wątpliwości. Zwłaszcza w tego typu przypadkach może dochodzić do sytuacji, w której współpracujące podmioty nie będą świadome występowania współadministrowania w relacji między nimi, a w konsekwencji będą naruszały przepisy z zakresu ochrony danych osobowych. Podobnie, jak w przypadku relacji pomiędzy administratorami a podmiotami przetwarzającymi, należy również wskazać, że nie można wykluczyć występowania relacji współadministrowania, jedynie na podstawie tego, że w danych okolicznościach jeden z podmiotów nie posiada faktycznego dostępu do przetwarzanych danych osobowych.

Wspólnie określone cele przetwarzania występują wtedy, gdy zaangażowane podmioty przetwarzają dane w tym samym celu albo wspólnym celu. Dodatkowo, w świetle orzecznictwa TSUE, relacja współadministrowania może powstać również, gdy zaangażowane podmioty realizują określone cele, które są ściśle powiązane lub się uzupełniają. Może tak być na przykład, kiedy z tej samej czynności przetwarzania wynika wzajemna korzyść dla zaangażowanych podmiotów, pod warunkiem, że każdy z nich uczestniczy w określaniu celów i sposobów relewantnej czynności przetwarzania.

Do zaistnienia współadministrowania zaangażowane podmioty muszą również wywierać wpływ na **sposoby przetwarzania**. Nie oznacza to jednak, że każdy z zaangażowanych podmiotów musi ustalać wszystkie sposoby przetwarzania – poszczególne podmioty mogą być zaangażowane na różnych etapach przetwarzania i w różnym zakresie. Należy przy tym uwzględnić to, który podmiot może faktycznie dokonywać określonych czynności (np. w sytuacji, gdy współadministratorzy korzystają ze standardowego narzędzia dostarczanego przez jednego z nich).

Na koniec rozważań dotyczących kwalifikacji podmiotów jako współadministratorów warto podkreślić, że podobnie, jak miało to miejsce w przypadku kwalifikowania podmiotów jako administratorów, należy opierać się na analizie konkretnych okoliczności przetwarzania danych, jako że pojęcie współadministrowania również jest pojęciem funkcjonalnym. Ponadto występują sytuacje, w których wprost w przepisach prawa wskazuje się, że określony podmiot posiada status współadministratora. W polskim systemie prawnym, takimi



przykładami są np. art. 24c ust. 1 ustawy o Państwowym Ratownictwie Medycznym oraz art. 10 ust. 5 ustawy o systemie powiadamiania ratunkowego.

Przykłady współadministrowania

Mając na uwadze powyższą kwalifikację oraz wytyczne właściwych organów można wskazać kilka przykładów sytuacji, w których będziemy mieli do czynienia ze współadministrowaniem.

- Dwie spółki stworzyły wspólnie produkt i organizują wydarzenie promocyjne dotyczące tego produktu. W tym celu wzajemnie udostępniają sobie dane dotyczące ich klientów oraz decydują, kto będzie zaproszony na wydarzenie. Ponadto uzgadniają również, w jakiej formie będą wysyłane zaproszenia, jak będą zbierane informacje zwrotne podczas wydarzenia oraz jakie będą podejmowane następcze działania marketingowe. Spółki te będą współadministratorami w zakresie działań związanych z organizowanym wydarzeniem promocyjnym.
- Agencja turystyczna, sieć hoteli i linia lotnicza wspólnie tworzą platformę internetową we wspólnym celu – oferowania pakietów turystycznych. Podmioty te wspólnie zdecydowały również o kluczowych sposobach przetwarzania, np. jakie dane będą przechowywane, w jaki sposób będą dokonywane i potwierdzane rezerwacje klientów oraz kto będzie miał dostęp do przechowywanych danych. Wskazane podmioty, w zakresie działalności związanej z platformą będą współadministratorami.
- Kilka instytutów badawczych zdecydowało się na przeprowadzenie wspólnego projektu badawczego, wykorzystując w tym celu istniejącą platformę jednego z instytutów biorącego udział w projekcie. Każdy z instytutów zasila tę platformę danymi osobowymi na potrzeby prowadzonego projektu oraz korzysta w ramach platformy z danych zamieszczanych tam przez pozostałe instytuty. Instytuty będą więc współadministratorami danych przetwarzanych w ramach platformy na potrzeby wspólnego projektu badawczego.

Konsekwencje zaistnienia relacji współadministrowania

Zakwalifikowanie określonej relacji jako współadministrowania rodzi określone skutki prawne dla współadministratorów. Dotyczy to zarówno obowiązków nałożonych na współadministratorów, jak i zakresu oraz zasad ponoszenia odpowiedzialności za działania niezgodne z przepisami z zakresu ochrony danych osobowych.

Współadministratorzy są zobowiązani w szczególności do poczynienia **wspólnych uzgodnień** określających zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

Współadministratorzy muszą więc ustalić między sobą, „kto za co odpowiada", tak aby zapewnić zgodność wspólnych operacji przetwarzania z przepisami RODO w tym odpowiednio wysoki poziom ochrony danych osobowych oraz unikanie sporów kompetencyjnych, które mogłyby doprowadzić do powstania luk w tej ochronie. W art. 26 ust. 1 RODO wskazano, że w ramach wspólnych uzgodnień współadministratorzy powinni dokonać podziału obowiązków **w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw na mocy RODO** (np. prawa dostępu do danych, usunięcia danych), oraz **obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO** (obowiązek informacyjny względem osób, których dane dotyczą). W uzgodnieniach współadministratorzy mogą podać wspólny punkt kontaktowy dla osób, których dane dotyczą.

Jak widać, wyliczenie to ma charakter przykładowy, a jednocześnie opisuje minimalny i obligatoryjny zakres wspólnych ustaleń. Wydaje się jednak, że najczęściej zasadne będzie ustalenie również wzajemnych ustaleń w zakresie spełniania pozostałych obowiązków wynikających z RODO, nałożonych na współadministratorów (jako jednego z typów administratorów). Współadministratorzy powinni więc wziąć pod uwagę w ramach wzajemnych ustaleń w szczególności obowiązki w zakresie:

- wdrożenia podstawowych zasad dotyczących przetwarzania danych osobowych (art. 5 RODO), np. zasady minimalizacji danych;
- zapewnienia odpowiedniej podstawy prawnej przetwarzania danych (art. 6 RODO); w wytycznych właściwych organów wskazuje się przy tym, że o ile to możliwe, współadministratorzy powinny opierać przetwarzanie danych osobowych na tożsamej podstawie prawnej;
- zapewnienia bezpieczeństwa przetwarzania (art. 32) poprzez stosowanie odpowiednich środków organizacyjnych i technicznych;
- informowania organu nadzorczego o naruszeniu ochrony danych osobowych oraz powiadamiania osób, których dane dotyczą o takim naruszeniu (art. 33 i 34 RODO);
- przeprowadzania ocen skutków dla ochrony danych (art. 35 i 36 RODO);
- korzystania z usług podmiotów przetwarzających (art. 28 RODO);
- transferu danych do państw trzecich (rozdział V RODO);
- kontaktowania się z osobami, których dane dotyczą oraz organem nadzorczym.

Jednocześnie należy wskazać, że tak jak samo istnienie relacji współadministrowania może wynikać wprost z przepisów prawa, tak również przepisy te mogą zawierać elementy wspólnych uzgodnień współadministratorów (tak jest przykładowo w przypadku wskazanego wyżej art. 24c ustawy o Państwowym Ratownictwie Medycznym). Warto podkreślić, że tego typu przepisy stanowią przejaw ograniczenia swobody współadministratorów w kształtowaniu zakresu swoich obowiązków oraz odpowiedzialności na drodze wspólnych ustaleń. Drugim ważnym ograniczeniem swobody współadministratorów w tym zakresie jest wskazany w art. 26 ust. 2 RODO wymóg, aby dokonane uzgodnienia należycie odzwierciedlały odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Przyjmuje się przy tym, że podziału odpowiedzialności na mocy wspólnych uzgodnień można dokonać co najmniej na dwa sposoby: według poszczególnych obowiązków lub według etapów przetwarzania. Dokonane uzgodnienia

powinny więc być odpowiednie i adekwatne do konkretnych operacji przetwarzania, które są dokonywane przez współadministratorów. Na przykład jeśli tylko jeden ze współadministratorów ma bezpośredni kontakt z osobami, zasadne będzie przypisanie mu realizacji obowiązku przekazania osobom, których dane dotyczą, wszelkich niezbędnych informacji dotyczących przetwarzania ich danych, zgodnie z art. 13 i 14 RODO.

RODO nie wskazuje, w jakiej formie uzgodnienia powinny zostać sporządzone (w przeciwieństwie np. do umowy powierzenia przetwarzania danych). Ze względu jednak na zasadę rozliczalności rekomendowane jest należyte udokumentowanie tych ustaleń.

Zasadnicza treść uzgodnień współadministratorów powinna być udostępniana osobom, których dane dotyczą. W RODO nie wskazano przy tym, co zawiera się w „zasadniczej treści uzgodnień". W wytycznych właściwych organów wskazuje się, że zasadnicza treść obejmuje informacje, o których mowa w art. 13 i 14 RODO oraz informacje o tym, który ze współadministratorów jest odpowiedzialny za zapewnienie zgodności przetwarzania z poszczególnymi elementami wskazanymi w wymienionych przepisach.

Co warto podkreślić, w RODO wprost wskazano także, że osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego ze współadministratorów, a więc niezależnie od poczynionych w tym zakresie ustaleń pomiędzy współadministratorami, w tym wskazanego punktu kontaktowego (art. 26 ust. 3 RODO).

Zakres odpowiedzialności współadministratorów

Dokonanie wspólnych ustaleń przez współadministratorów stanowi zarówno jednocześnie uprawnienie współadministratorów, jak i ich obowiązek. Niedochowanie tego obowiązku może skutkować ponoszeniem odpowiedzialności przewidzianej w RODO. Naruszenie art. 26 RODO może skutkować w szczególności nałożeniem kary pieniężnej w wysokości do 10 mln euro albo w wysokości do 2% całkowitego rocznego światowego obrotu administratora (art. 83 ust. 4 lit. a) RODO).

Ponadto współadministratorzy, jako jeden z typów administratorów, mogą odpowiadać za naruszenie każdego innego obowiązku nałożonego na administratorów, które są wskazane w RODO.

W kontekście odpowiedzialności współadministratorów należy wskazać również na przewidzianą w RODO możliwość ponoszenia odpowiedzialności cywilnoprawnej, zgodnie z art. 82 RODO. Na podstawie tego przepisu każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. W kontekście współadministrowania ważna jest przy tym zasada, że jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator (a tak jest m.in. w przypadku współadministrowania) lub podmiot przetwarzający i odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni **odpowiedzialność solidarną za całą szkodę**, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania (art. 82 ust. 4 RODO). Administrator (lub podmiot przetwarzający), który zapłacił odszkodowanie za całą wyrządzoną szkodę, ma **prawo żądania od pozostałych administratorów lub podmiotów przetwarzających**, którzy uczestniczyli w tym samym przetwarzaniu, **zwrotu części odszkodowania** odpowiadającej części szkody, za którą ponoszą odpowiedzialność.

Bartosz Jussak
radca prawny w kancelarii Barta & Kaliński sp. j.; specjalizuje się w projektach związanych z prawem nowych technologii, prawem własności intelektualnej oraz ochroną danych osobowych

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) (Dz. Urz. UE. L. z 2016 r. Nr 119, s. 1 z późn. zm.).
2 Por. w szczególności: Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 (wersja przedstawiona do publicznych konsultacji), s. 13–14.
3 Por. Guidelines 07/2020 on the concepts… s. 18 i wskazane tam orzecznictwo.
4 Por. Guidelines 07/2020 on the concepts… s. 19 i wskazane tam orzecznictwo.
5 Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (t.j. Dz.U. z 2020 r. poz. 882 z późn. zm.).
6 Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (t.j. Dz.U. z 2021 r. poz. 268).
7 Por. Guidelines 07/2020 on the concepts…
8 Por. Guidelines 07/2020 on the concepts… s. 41.
9 Tak: I. Kowalczyk-Pakuła, M. Chołuj, Współadministrowanie – nowy paradygmat w prawie ochrony danych osobowych (dodatek Monitor Prawniczy 21/2019) w: „Prawo nowych technologii dane osobowe i cyberbezpieczeństwo, Internet i media, handel elektroniczny, prawo IT, technologie" pod red. Xawerego Konarskiego.
10 Por. Guidelines 07/2020 on the concepts… s. 44.

Polityka prywatności na stronach internetowych

Jak właściwie spełnić obowiązek informacyjny?

Joanna Legun

Dziś, szczególnie w dobie pandemii koronawirusa, przedsiębiorcy coraz chętniej przenoszą swoje biznesy do internetu. Przedsiębiorcy inwestują w strony internetowe, żeby pozyskiwać nowych klientów, otwierać sklepy internetowe, budować listę mailingową czy po prostu być widocznym w sieci.

Powyższe jest ściśle związane z przetwarzaniem danych osobowych, a to powoduje, że przedsiębiorca musi zmierzyć się z szeregiem zagadnień związanych z tym obszarem, w tym np. z polityką prywatności. Ci, którzy dopiero zaczynają działać w sieci, często zastanawiają się, czy na swojej stronie internetowej potrzebują umieścić politykę prywatności i w jakim zakresie dotyczą ich przepisy o ochronie danych osobowych.

Czym jest RODO?

Zacznijmy od wytłumaczenia, co kryje się pod powszechnie używanym skrótem RODO. Jest to 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). Nazwa jest długa i skomplikowana – stąd powszechnie używa się dla niej skrótowego określenia RODO.

RODO obowiązuje od 25 maja 2018 roku, czyli już od prawie 3 lat. Jednak do dziś budzi ono sporo wątpliwości, a niektórych przedsiębiorców przyprawia o szybsze bicia serca.

Przede wszystkim rozporządzenie o ochronie danych osobowych stosujemy bezpośrednio. To znaczy, że jeżeli przedsiębiorca chce sprawdzić, jakie obowiązki w zakresie przetwarzania danych osobowych nakłada na niego RODO, to powinien spojrzeć bezpośrednio do tego aktu, a nie polskiej ustawy. Jest to jeden z nielicznych przypadków, gdzie instytucje unijne zdecydowały się na uregulowanie kwestii prawnych w rozporządzeniu, a nie dyrektywie, która wymaga implementacji do polskiego porządku prawnego.

RODO ma zapewnić bezpieczeństwo i spójność przetwarzania danych osobowych. Nakłada ono na administratora danych osobowych szereg obowiązków, w tym właśnie konieczność spełnienia wobec osób, których dane osobowe są przetwarzane, obowiązków informacyjnych, czyli poinformowanie ich, co administrator danych osobowych będzie robił z zebranymi od nich danymi osobowymi.

Ale czy RODO dotyczy także małego przedsiębiorcy, który zakłada sklep internetowy czy stronę – wizytówkę swojego biznesu?

Czy przedsiębiorca na stronie internetowej musi stosować RODO?

Jeszcze przed wejściem w życie RODO można było spotkać przedsiębiorców, którzy pewni siebie mówili, że ich przepisy dotyczące przetwarzania danych osobowych czy ich bezpieczeństwa nie dotyczą. Oni przecież nie zbierają żadnych danych osobowych.

Dziś, po kilku latach obowiązywania RODO, świadomość obowiązków przedsiębiorców wynikających z przetwarzania danych osobowych jest o wiele większa. Jednak mimo wszystko co jakiś czas pada pytanie z ust osób planujących prowadzić działalność nierejestrowaną, czy ich RODO naprawdę dotyczy.

W praktyce trudno jest sobie wyobrazić przedsiębiorcę, który nie przetwarza w ogóle danych osobowych. Bo przecież przedsiębiorca pozyskuje klientów, odpowiada na maile w sprawie ofert, ma pracowników czy chociażby ma listę osób zapisanych na jego newsletter. Do tych wszystkich czynności potrzebne są przecież dane osobowe – adresy e-mail, numery telefonów czy imiona i nazwiska klientów.

RODO nie stosuje się do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Trudno uznać, że prowadzenie działalności nierejestrowanej czy pozyskiwanie danych osobowych na stronie internetowej będzie tym wyjątkiem. Tym bardziej że wyjątek trzeba interpretować bardzo wąsko. Przedsiębiorca pozyskuje dane osobowe po to, żeby prowadzić działalność gospodarczą – nie jest to osobisty czy domowy charakter.

Przedsiębiorca jako administrator danych osobowych

Przedsiębiorca, który na przykład prowadzi sklep internetowy staje się administratorem danych osobowych między innymi swoich klientów. Zgodnie z definicją administratora danych osobowych ujętą w RODO, administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Zgodnie z tą definicją administratorem danych osobowych może być na przykład spółka z ograniczoną odpowiedzialnością czy osoba fizyczna prowadząca jednoosobową działalność gospodarczą. Nie można utożsamiać administratora

na przykład z członkiem zarządu spółki z ograniczoną odpowiedzialnością, pracownikiem spółki czy prokurentem osoby, która prowadzi jednoosobową działalność gospodarczą.

Administrator dodatkowo samodzielnie ustala cele i sposoby przetwarzania danych osobowych. Co to w praktyce oznacza? Jeżeli przedsiębiorca chce prowadzić sklep internetowy z zabawkami, to jasne jest, że podczas sprzedaży swoich towarów będzie pozyskiwał dane osobowe klientów. A zatem samodzielnie określa, w jakim celu będzie zbierał dane osobowe – w tym przypadku celem będzie realizacja umowy sprzedaży zabawek. Dodatkowo ten sam sprzedawca będzie decydował, jakie będą sposoby przetwarzania tych danych osobowych – tzn. sam określi, co będzie się działo z danymi osobowymi jego klienta.

W takim właśnie przypadku sprzedawca staje się administratorem danych osobowych swojego klienta, a co za tym idzie – ma wiele obowiązków, które nakłada na niego RODO. To właśnie administrator jest odpowiedzialny za bezpieczeństwo danych osobowych, które posiada.

Dane osobowe, które mogą być pozyskiwane na stronie internetowej

Sposobów pozyskiwania danych osobowych na stronie internetowej może być więcej – nie tylko będzie to realizacja umowy sprzedaży.

Przedsiębiorca może stać się administratorem danych osobowych, pozyskiwanych na stronie internetowej, w związku z następującymi procesami:

a) zapisem na newsletter,
b) korzystaniem z formularza kontaktowego,
c) prośbą o przedstawienie oferty,
d) zawarciem i realizacją umowy,
e) zapisaniem się na listę osób oczekujących na produkt,
f) umieszczeniem komentarza pod wpisem na blogu.

Powyższe wyliczenie ma charakter przykładowy. Nie na każdej stronie internetowej administrator będzie pozyskiwał dane osobowe na wszystkie podane wyżej cele. Administrator może pozyskiwać dane osobowe na realizację jeszcze innych celów.

Polityka prywatności a RODO

Polityka prywatności to pojęcie, które jednoznacznie kojarzy się z RODO. Natomiast w samej treści rozporządzenia nie pojawia się jego wytłuczenie. Co więcej – określenie polityka prywatności nie zostaje w nim użyte ani razu. Skąd więc taka popularność polityk prywatności?

RODO nakazuje spełniać wobec osób, których dane osobowe przetwarza administrator, tzw. obowiązki informacyjne. Na stronie internetowej może być kilka miejsc, w których odwiedzający może przekazać swoje dane osobowe przedsiębiorcy. Administrator dla każdego procesu może stworzyć osobny obowiązek informacyjny i umieścić go w odpowiednim miejscu na stronie internetowej.

Na przykład osoba, która odwiedza stronę internetową, chce zapisać się na newsletter, zostawić komentarz na blogu czy poprosić o przedstawienie oferty. Każdy z tych celów przetwarzania jest inny, a co za tym idzie, inne będą również obowiązki informacyjne. Różnić się mogą one na przykład podstawą prawną przetwarzania czy celem przetwarzania. Bez wątpienia przedsiębiorcy łatwiej będzie zebrać wszystkie obowiązki w jednym dokumencie, który będzie dotyczył zarówno zapisu na newsletter, jak i komentarza na blogu czy żądania przedstawienia oferty niż opracować kilka odrębnych obowiązków informacyjnych i rozmieszczać je w różnych miejscach na stronie internetowej.

Łatwiej jest też administratorowi opanować proces spełniania obowiązków informacyjnych, jeżeli wszystko znajduje się w jednym miejscu. I to z tych powodów polityka prywatności będąca jednym dokumentem, który zawiera w sobie wszystkie informacje o przetwarzaniu danych osobowych, jest tak popularna.

Treść obowiązku informacyjnego

Lista informacji, która powinna znaleźć się w obowiązku informacyjnym wynika z art. 13 RODO. Niestety lista jest długa, a administrator jest obowiązany

Lista informacji, która powinna znaleźć się w obowiązku informacyjnym wynika z art. 13 RODO.

do podania wszystkich informacji, które znajdują się na tej liście.

Jednak jest też dobra wiadomość. Część z informacji, które administrator powinien przekazać swojemu klientowi, jest stałych. To znaczy, że taka sama treść znajdzie się zarówno w obowiązku informacyjnym dla osób, które chcą się zapisać na newsletter, jak i tych, które proszą o przedstawienie oferty czy korzystają z usług przedsiębiorcy.

Zacznijmy od tych informacji, które będą takie same w każdym obowiązku informacyjnym.

Po pierwsze, administrator powinien podać swoją tożsamość oraz dane kontaktowe. Osoby, które dopiero zaczynają prowadzić jednoosobową działalność gospodarczą, często mają problem z podaniem swojego imienia i nazwiska oraz adresu prowadzenia działalności. Chcą ograniczyć się do podania marki, pod którą działają. Jest to niestety błąd. Osoba, która powierza administratorowi swoje dane osobowe, powinna znać imię i nazwisko administratora.

Po drugie, administrator powinien wskazać dane inspektora ochrony danych osobowych, ale tylko wtedy, gdy powołał on kogoś na to stanowisko. W praktyce obowiązek powołania inspektora rzadko dotyka drobnych czy początkujących przedsiębiorców.

Po trzecie, administrator powinien również poinformować osobę, której dane pozyskuje, o prawach jej przysługujących, czyli o prawie do:

a) żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
b) sprostowania danych osobowych,
c) usunięcia lub ograniczenia przetwarzania danych osobowych,
d) wniesienia sprzeciwu wobec przetwarzania,
e) przenoszenia danych,
f) wniesienia skargi do organu nadzorczego, czyli Prezesa Urzędu Ochrony Danych Osobowych.

Wskazane powyżej trzy elementy w każdym obowiązku informacyjnym będą takie same. Natomiast kolejna grupa informacji, którą należy podać w obowiązkach informacyjnych, powinna być dostosowana do konkretnego celu przetwarzania danych osobowych.

Po pierwsze, administrator powinien wskazać cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania.

Gdy przedsiębiorca przetwarza dane klienta, który kupił w jego sklepie internetowym zabawki, to celem przetwarzania danych osobowych będzie realizacja umowy sprzedaży, a podstawą prawną przetwarzania będzie umowa sprzedaży zawarta między administratorem danych osobowych a klientem. W przypadku zapisu na newsletter celem przetwarzania danych osobowych może być właśnie wysyłka newslettera, a podstawą do przetwarzania danych osobowych może być zgoda osoby, której dane dotyczą.

Dodatkowo jeżeli administrator wskazuje, że podstawą przetwarzania danych osobowych jest prawnie uzasadniony interes administratora lub osoby trzeciej, to również powinien jasno wskazać, na czym polega ten uzasadniony interes.

Gdy podstawą prawną przetwarzania danych osobowych jest zgoda, to również w obowiązku informacyjnym powinna znaleźć się informacja o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Po drugie, administrator powinien wskazać informacje o odbiorcach danych lub o kategoriach odbiorców, którym dane mogą być przekazywane. I tu również w przypadku każdej z grup katalog podmiotów może być różny. Na przykład dane osób, które zrobiły zakupy w sklepie internetowym, administrator może przekazać do firmy księgowej w celu wykonania rozliczeń. Natomiast adresy e-mail osób zapisanych na listę newsletterową mogą być przetwarzane na polecenie administratora przez firmę świadczącą usługi wysyłki i zarządzenia newsletterem.

Po trzecie, jeżeli przedsiębiorca chce przekazać dane do państw poza Europejskim Obszarem Gospodarczym (EOG) lub do organizacji międzynarodowej, to powinien umieścić również odpowiednią informację o tym procesie. W szczególności przedsiębiorca powinien zwrócić uwagę czy np. serwery, na których przechowuje swoje dane osobowe, nie znajdują się poza EOG.

Po czwarte, administrator powinien również poinformować osobę, której dane osobowe zamierza przetwarzać, jak długo dane osobowe będą przechowywane. Jeżeli ustalenie konkretnej daty jest niemożliwe, to administrator powinien poinformować, jakie są kryteria ustalania tego okresu. Tu również przez inny okres przedsiębiorca musi przechowywać dane związane ze sprzedażą jego usług w przez inny okres może przechowywać dane osób zapisanych na newsletter.

Po piąte, w obowiązku informacyjnym powinna znaleźć się również informacja, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy. Ponadto administrator powinien poinformować, czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych. Te informacje także będą inaczej się kształtować w zależności od tego, w jakim celu dane osobowe będą przetwarzane.

Po szóste, w obowiązku informacyjnym powinny się również znaleźć informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu – oczywiście o ile administrator będzie prowadził takie działania na danych osobowych.

Sposób spełnienia obowiązku informacyjnego

W przypadku pozyskania danych osobowych na stronie internetowej administrator danych osobowych powinien spełnić obowiązek informacyjny w momencie

pozyskania danych osobowych. W praktyce przedsiębiorcy w formularzach, gdzie pozyskują dane osobowe, umieszczają dodatkowy checkbox z oświadczeniem, że osoba zapoznała się z treścią polityki prywatności. Bez zaznaczenia tej informacji nie można sfinalizować zakupu czy skutecznie zapisać się na newsletter.

Ponadto przedsiębiorca powinien pamiętać, żeby treść polityki była jasna i przejrzysta dla odbiorców. Nie chodzi tu tylko o kwestię słownictwa użytego w polityce, ale również wizualną treść polityki. Trudno będzie klientom zapoznać się z treścią obowiązków informacyjnych, gdy będą one umieszczone małą czcionką na mało odróżniającym się tle. Dla wygody czytelnika można również wprowadzić śródtytuły. Dobrą praktyką jest również tworzenie polityki prywatności w formie pytań i odpowiedzi.

Jeżeli przedsiębiorca komunikuje się ze swoimi odbiorcami również w innym języku niż polski, to warto, żeby treść polityki była dostępna również w innym języku. Na przykład tłumacz przysięgły języka angielskiego świadczy usługi zarówno dla osób, które posługują się językiem polskim, jak i angielskim. Strona internetowa ma dwie wersje językowe – polską i angielską. Stąd tłumacz powinien umieścić na swojej stronie również politykę prywatności w języku polskim i angielskim.

Aktualizacja polityki prywatności

Jeżeli przedsiębiorca umieścił na stronie internetowej politykę prywatności, to nie oznacza, że może spocząć na laurach i całkowicie zapomnieć o procesie przetwarzania danych osobowych.

Treść obowiązków informacyjnych zawartych w polityce prywatności przedsiębiorca powinien dostosować do swojego procesu przetwarzania danych osobowych. Stąd jeżeli zmienią się jakieś informacje zawarte w obowiązku informacyjnym, to należy zaktualizować treść polityki. Na przykład mogą zmienić się dane przedsiębiorcy, czyli jego adres czy numer telefonu albo zakres podmiotów, którym dane osobowe będą przekazywane.

Drugą kwestią, na którą przedsiębiorca powinien zwrócić uwagę, jest to, czy na skutek na przykład wprowadzenia zmian na stronie internetowej czy aktualizacji zainstalowanych wtyczek osoby, które korzystają ze strony internetowej, mogą bez problemów zapoznać się z treścią polityki prywatności. Kilkakrotnie spotkałam się z sytuacją, że link do polityki prywatności odsyłał mnie do nieistniejącej strony internetowej.

Czy polityka prywatności to koniec obowiązków nałożonych na przedsiębiorcę w związku z przetwarzaniem danych osobowych?

Niestety często przedsiębiorcy myślą, że spełnienie obowiązku informacyjnego czy umieszczenie polityki prywatności na stronie internetowej to koniec obowiązków jakie nakłada na nich RODO. A jest to tylko szczyt góry lodowej.

Spełnienie obowiązku informacyjnego to działanie, które klienci przedsiębiorcy mogą samodzielnie dostrzec. Jeżeli klient zapisuje się na newsletter, a nie ma możliwości przeczytać, co się będzie działo z jego danymi osobowymi, to od razu dostrzeże, że przedsiębiorca nie realizuje obowiązków wynikających z RODO.

Natomiast ta sama osoba, która zapisuje się do newslettera na pierwszy rzut oka nie może zweryfikować, czy przedsiębiorca faktycznie realizuje uprawnienia osób zapisanych do newslettera, czy i z kim ma zawarte umowy powierzenia przetwarzania danych osobowych, czy przetwarzane przez niego dane osobowe są bezpieczne itd. RODO to nie tylko polityka prywatności i obowiązki informacyjne – to cały proces zapewnienia przez administratora bezpieczeństwa przetwarzania danych osobowych i wprowadzenie licznych procedur, które mają za zadanie zrealizować ten cel.

Joanna Legun
adwokat, specjalizuje się w sporach sądowych oraz ochronie danych osobowych; prowadzi stronę internetową pod adresem www.jakzrozumiecprawnika.pl, gdzie publikuje artykuły wyjaśniające zagadnienia prawne istotne dla przedsiębiorców

Otwarte dane filarem innowacyjnej gospodarki

Co przyniesie nowa ustawa?

Michał Nowakowski

Jednym z warunków rozwoju cyfrowego jest szybki i efektywny dostęp do danych wysokiej jakości, które pozwalają na tworzenie bardziej innowacyjnych rozwiązań, m.in. w obszarze tzw. sztucznej inteligencji czy też, ujmując to bardziej precyzyjnie, automatyzacji i predykcji. W Europejskiej Strategii w zakresie danych, która została opracowana przez Komisję Europejską, wskazano otwartość wysokiej jakości i wartości danych jako jeden z filarów budowania konkurencyjności gospodarki Unii Europejskiej. W związku z tym w 2021 r. zostało zaplanowane przyjęcie aktów wykonawczych, które umożliwią udostępnianie przez szeroko rozumiany sektor publiczny zbiorów danych w formacie nadającym się do odczytu maszynowego (ang. *machine-readable*) oraz za pośrednictwem interfejsów programowania aplikacji (*API*). Otwartość danych jest wskazywana jako kluczowy element do pobudzenia innowacji w wielu sektorach gospodarki, ale także w nauce, a technologie uczenia maszynowego, przetwarzanie języka naturalnego czy internet rzeczy wymagają zwiększenia podaży wspomnianych danych.

W pewnym uproszczeniu można stwierdzić, że realizacja projektu otwartych danych (ang. *open data)* została zapoczątkowana przez przyjęcie Dyrektywy 2019/1024 w sprawie otwartych danych i ponownego wykorzystania informacji sektora publicznego[2] (dalej: DOD). Ma ona zostać implementowana do krajowego porządku prawnego nie później niż 17 lipca 2021 r. Polski ustawodawca od kilku miesięcy prowadzi prace nad przyjęciem ustawy o takim samym tytule jak powyższa dyrektywa.

Czytelnik powinien zatem zwrócić uwagę na następujące kwestie:

1. istotność tematyki otwartych danych w kontekście rozwoju innowacji cyfrowych oraz powiązanych z tym tzw. *business opportunities*;
2. wysoki poziom ochrony prawnej danych i związane z tym ograniczenia, również dla podmiotów zamierzających skorzystać z nowych możliwości;
3. perspektywy, które mogą zostać wykreowane w przyszłości w związku z realizacją Europejskiej Strategii dla danych.

Nie można jednocześnie zapominać o tym, że otoczenie prawno-regulacyjne w zakresie danych podlega nieustannym i dynamicznym zmianom, a także że w odniesieniu do niektórych sektorów oraz technologii mogą pojawiać się dodatkowe wymogi, np. w kontekście przejrzystości i wyjaśnialności algorytmów. Jest to o tyle istotne, że większość aktów prawnych, tworzonych na potrzeby realizacji założeń strategicznych dla cyfrowej Europy, jest pisana w sposób neutralny technologicznie, tj. brakuje im jednoznacznego określenia technologii, pozostawiając po stronie beneficjenta (wykorzystującego) decyzję co do sposobu wykorzystania tych rozwiązań, przy zastrzeżeniu, że ten musi przeprowadzić stosowną analizę ryzyka tzw. *risk-based approach*.

I na koniec wstępu ważna informacja – ponowne wykorzystanie danych sektora publicznego nie powinno być utożsamiane z dostępem do informacji publicznej. Choć są to pojęcia do siebie zbliżone, to ich ostateczne cele są zgoła odmienne.

Otwarte dane i ponowne wykorzystywanie informacji sektora publicznego

Na dzień 16 marca 2021 r. nadal trwały prace nad projektem wspomnianej wcześniej ustawy. Ma ona być – wraz z projektem Rozporządzenia w sprawie europejskiego zarządzania danymi (*Data Governance Act*) – punktem wyjścia do przybliżenia możliwości, warunków i ograniczeń związanych z *open data*.

Zanim jednak przejdziemy do omawiania tych dwóch aktów, spójrzmy na założenia samej DOD. Jej ogólną zasadą jest to, że państwa członkowskie mają zapewnić możliwość ponownego wykorzystania dokumentów określonych w dyrektywie do celów komercyjnych lub niekomercyjnych. Jeżeli chodzi o zakres tych dokumentów, to zostały one określone dosyć szeroko. Można tutaj wskazać m.in. na te będące w posiadaniu sektora publicznego (i pokrewnych) czy danych badawczych. Jednocześnie zarówno dyrektywa, jak i projektowana ustawa czy rozporządzenie zawierają liczne wyłączenia, które w uproszczeniu są pochodną konieczności zapewnienia bezpieczeństwa konkretnych danych.

Jak obowiązek udostępnienia danych będzie realizowany przez nową ustawę?

W art. 5 projektu ustawy znajdziemy stwierdzenie, że każdemu przysługuje prawo do ponownego wykorzystania informacji sektora publicznego, czyli informacji:

1. udostępnionych na stronie Biuletynu Informacji Publicznej podmiotu zobowiązanego lub na portalu danych lub w innym systemie teleinformatycznym podmiotu zobowiązanego;
2. przekazanych na wniosek o ponowne wykorzystywanie.

Jednocześnie w projekcie ustawy znajdziemy pewne kategorie danych, których ponowne wykorzystanie może

doznawać modyfikacji korzystnych dla użytkowników, m.in. ze względu na ich wartość. Mowa tutaj o:

- danych o wysokiej wartości (istotnych z punktu widzenia m.in. społeczeństwa, środowiska czy gospodarki),
- danych dynamicznych (szybko się dezaktualizujących),
- danych badawczych (z pewnymi ograniczeniami),

które zostały opisane w rozdziale 5 projektu ustawy. Kwestie te omówimy w dalszej części artykułu.

Definicja

Z punktu widzenia omawianego zagadnienia istotna jest również definicja otwartych danych, zawarta w projekcie ustawy. Istotna przede wszystkim ze względu na to, że wskazuje, jakiego rodzaju dane powinny być udostępniane przez podmioty publiczne oraz w jaki sposób będą one udostępnianie przez zobowiązane podmioty. Zgodnie z projektowaną ustawą otwartymi danymi są informacje sektora publicznego udostępniane lub przekazywane w postaci elektronicznej, kompletne, aktualne, niezastrzeżone, w wersji źródłowej, w otwartym formacie przeznaczonym do odczytu maszynowego, do bezpłatnego ponownego wykorzystywania na tych samych zasadach dla każdego użytkownika, bezwarunkowo lub z zastrzeżeniem warunków dla danych, o których mowa była we wcześniejszym akapicie.

Jednocześnie dane podlegają też pewnym wyłączeniom z obowiązku udostępniania. Chodzi o dane wskazane w art. 4 ustawy (pełen katalog), czyli m.in. o informacje będące w posiadaniu jednostek publicznej radiofonii i telewizji, państwowych i samorządowych instytucji kultury (z pewnymi wyłączeniami), uczelni czy szkół, bibliotek naukowych, a także niektórych podmiotów o charakterze komercyjnym, jeżeli nie są to informacje wytworzone w zakresie zadań publicznych. Powyższe wyłączenie nie obejmuje tych danych, które podlegają obowiązkowemu ujawnieniu w Biuletynie Informacji Publicznej.

Informacje sektora publicznego, których udostępnienie lub przekazanie zostało uzależnione od wykazania przez użytkowników interesu prawnego lub faktycznego na podstawie odrębnych przepisów, również nie podlegają przepisom projektowanej ustawy.

To jednak nie koniec ograniczeń. Zgodnie z art. 6 projektu ustawy prawo do ponownego wykorzystania podlega także ograniczeniom wynikającym z przepisów o ochronie informacji niejawnych czy ochronie innych tajemnic ustawowo chronionych (np. tajemnica zawodowa związana z wykonaniem pracy w organie administracji). Dodatkowo wnioskodawca nie otrzyma informacji dotyczącej tajemnicy przedsiębiorstwa (chyba, że zostanie wyrażona zgoda na jej niestosowanie) czy prywatności osoby fizycznej, ale z wyjątkiem informacji dotyczących osób pełniących funkcje publiczne czy na podstawie zgody osoby fizycznej na przetwarzanie danych. Takie same ograniczenia rozciągają się także na informacje, do których dostęp jest ograniczony na podstawie innych przepisów (np. ze względu na objęcie ich ochroną na podstawie innych przepisów).

Istotny jest też art. 6 ust. 4, który wskazuje, że podobne ograniczenia dotyczą także m.in. informacji objętych prawami własności przemysłowej czy programy komputerowe (z zastrzeżeniem art. 10 ust. 5). W rzeczywistości katalog ten jest jednak znacznie szerszy.

Na marginesie warto też zauważyć, że dodatkowe warunki w zakresie udostępniania i wykorzystywania danych będą mogły wynikać (zarówno dla podmiotu zobowiązanego, jak i wnioskodawcy) z projektowanego *Data Governance Act*, którego zapisy będzie się stosować do informacji objętych:

1. tajemnicą handlową,
2. poufnością informacji statystycznych,
3. przepisami o ochronie praw własności intelektualnej osób trzecich,
4. przepisami o ochronie danych osobowych.

Szersza analiza będzie jednak możliwa dopiero po przyjęciu tego aktu w określonej formie.

Kto będzie zobowiązany do stosowania ustawy?

Zakres podmiotowy jest dosyć szeroki i wyznacza go treść art. 3 projektu ustawy[3].

Na początku konieczna jest jedna uwaga dotycząca zależności pomiędzy ustawą a projektowanym Rozporządzeniem w sprawie europejskiego zarządzania danymi. Ten drugi akt posługuje się pojęciem organu sektora publicznego oznaczającego państwo, władze regionalne lub lokalne, podmioty prawa publicznego lub związki złożone z co najmniej jednej

takiej instytucji lub z co najmniej jednego takiego podmiotu prawa publicznego. Z kolei w projekcie ustawy posłużono się definicją, w której enumeratywnie wymieniono konkretne podmioty.

Są nimi m.in. jednostki sektora finansów publicznych, państwowe jednostki organizacyjne nieposiadające osobowości prawnej czy osoby prawne utworzone w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, których działalność nie ma charakteru przemysłowego lub handlowego, ale które jednocześnie spełniają pewne dodatkowe wymagania (art. 3 ust. 1 pkt 3). Do katalogu tego zalicza się więc przedsiębiorstwa państwowe czy podmioty wykonujące tzw. działalność sektorową, np. w obszarze energetyki.

Zasady udostępniania i przekazywania informacji sektora publicznego

Udostępnianie danych podlega naczelnej zasadzie równości, tj. są one udostępniane w porównywalnych warunkach i na takich samych zasadach, a dodatkowo niedopuszczalne jest – co do zasady – wprowadzanie ograniczeń w wykorzystaniu danych. Z tym jednak zastrzeżeniem, że dopuszczalne jest zawarcie umowy na wyłączność, jeżeli wymaga tego prawidłowe wykonywanie zadań publicznych – Ustawa bardziej szczegółowo określa zasady dotyczące tego typu umów.

metadanymi, czyli ustrukturyzowanymi informacjami opisującymi, tłumaczącymi, lokalizującymi i ułatwiającymi odnalezienie, wykorzystanie lub zarządzanie informacjami – dane o danych. Warto tutaj wskazać, że Komisja Europejska w swoim *Rolling Plan for ICT standardisation* również wskazuje na potrzebę standaryzacji formatów danych czy taksonomii.

Pewnym zaskoczeniem może być jednak to, że podmiot zobowiązany nie jest zobligowany do tworzenia informacji w sposób określony w stosownym wniosku (o czym w dalszej części), jeżeli spowoduje to konieczność podjęcia nieproporcjonalnych działań przekraczających proste czynności. Pozostawia to sporą sferę dyskrecjonalną podmiotowi publicznemu, choć oczywiście podlegającej ocenie w odniesieniu do danego stanu faktycznego. Bardzo korzystne jest też to, że podmiot publiczny może udostępnić lub przekazać nie tylko same informacje, ale także kod źródłowy czy inne elementy programu komputerowego opracowanego w ramach realizacji zadań publicznych. Jest to w pewnym sensie forma wdrożenia w życie idei Open Source, która jest dosyć popularna w programistycznym świecie.

Upraszczając, o tym czy dany podmiot jest podmiotem zobowiązanym, czy też nie, w rozumieniu Ustawy, będzie decydować zasadniczo:

1. zaliczenie do kategorii wskazanej w art. 3 Ustawy,
2. wyłączenie ze stosowania Ustawy – w kontekście posiadanych informacji objętych ograniczeniami lub
3. zaliczenie do katalogu określonego w projektowanym Rozporządzeniu *Data Governance*, w szczególności wyłączenie na podstawie art. 3 pkt 2).

Analizując zakres podmiotowy, można dojść do wniosku, że wyznaczenie tego kręgu jest skomplikowane. Dla uproszczenia można więc przyjąć, że chodzi o podmioty sektora publicznego, a ewentualne ograniczenia będą wynikały z przepisów omawianej ustawy lub odrębnych przepisów.

Jak już wspomniano, zasadą, która została wyrażona w art. 10 ustawy, jest udostępnianie i przekazywanie danych jako otwartych danych. Przy czym dane te mogą być udostępniane – i zazwyczaj pewnie będą – z użyciem systemów ICT (teleinformatycznych), w tym również przy użyciu programistycznych interfejsów dostępowych – API, które można przyrównać do wtyczki, do której wkładamy drugą końcówkę w celu uzyskania połączenia. W takiej sytuacji podmiot publiczny zobowiązany jest do:

1. stosowania formatów danych oraz
2. protokołów komunikacyjnych i szyfrujących,

które zostały określone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne[4]. O ile to możliwe dane powinny być udostępnione w formacie przeznaczonym do odczytu maszynowego i wraz z tzw.

Pojawia się pytanie, gdzie znaleźć będzie można informacje o danych podlegających Ustawie. Art. 11 przewiduje, że w Biuletynie Informacji Publicznej w odpowiednim menu przedmiotowym powinna znaleźć się kategoria „Ponowne wykorzystanie", która ma zawierać szereg elementów, w tym m.in. informacje nt. warunków ponownego

wykorzystania (traktowane jako ofertę), o wysokości opłat za ponowne wykorzystanie, a także o środkach odwoławczych. Dopuszczalne jest także udostępnienie danych na tzw. portalu danych i w takiej sytuacji informacja o tym powinna znaleźć się w stosownej zakładce.

I ważna informacja – brak informacji to dobra informacja. Oznacza, że udostępnienie nie podlega żadnym dodatkowym warunkom.

Warunki ponownego wykorzystania

Zasadniczo informacje sektora publicznego udostępniane są lub przekazywane w celu ich ponownego wykorzystania bezwarunkowo. Przy czym podmiot zobowiązany do udostępnienia **może** określić warunki **ponownego wykorzystania,** stosując otwarte licencje. Jeżeli natomiast dane zawierają informacje stanowiące dane osobowe, podmiot zobowiązany ma obowiązek określić takie warunki ponownego wykorzystania. W praktyce jednak przepis został określony w sposób na tyle otwarty, że de facto podmiot każdorazowo może określić warunki ponownego wykorzystania.

W Ustawie określono, że warunki powinny być obiektywne, proporcjonalne, niedyskryminacyjne i nie mogą w nieuzasadniony sposób ograniczać możliwości ponownego wykorzystania. Oczywiście z zastrzeżeniem, kiedy jest to uzasadnione wspomnianym już prawidłowym wykonaniem zadań publicznych.

Ustawa wprowadza jednak pewne ograniczenia co do zakresu tych warunków. Mogą one dotyczyć bowiem jedynie trzech obszarów, tj.:

1. obowiązku umieszczenia informacji o źródle, czasie wytworzenia i pozyskania informacji,
2. obowiązku informowania o przetworzeniu informacji ponownie wykorzystywanej oraz
3. zakresu odpowiedzialności podmiotu przekazującego lub udostępniającego.

Jak wspomnieliśmy już wcześniej – pewne kategorie danych podlegają szczególnym zasadom. Na przykład dane badawcze, będące w posiadaniu m.in. uniwersytetów, podlegają ponownemu wykorzystaniu jedynie wtedy, gdy są finansowane ze środków publicznych oraz zostały już publicznie udostępnione w systemie takiego podmiotu (np. na portalu zawierającym takie zbiory danych). W tym przypadku dane udostępnia się bezpłatnie. Pewne ograniczenia mogą się pojawić po wydaniu stosownego rozporządzenia (art. 22).

Warunki udostępniania danych dynamicznych przytoczonych na początku artykułu, jak np. danych z czujników mogących wykorzystywać przykładowo dane biometryczne (tutaj mamy oczywiście dodatkowe wymogi związane z RODO), również zostały określone specyficznie, tj.:

1. podlegają one udostępnieniu niezwłocznie po ich zgromadzeniu,
2. mają być udostępnione za pośrednictwem interfejsu dostępowego API oraz
3. muszą być przysposobione do zbiorczego pobrania – o ile to możliwe (założyć można, że zgodnie z pozostałymi zasadami udostępniania danych, jeżeli ich udostępnienie w tej formie będzie wiązało się z nadmiernymi kosztami lub trudnościami, to nie będzie takiego obowiązku).

Powyższe jest o tyle zasadne, że w Ustawie przewidziano również, że niezwłoczne udostępnienie danych dynamicznych może zostać odłożone w czasie, jeżeli ich udostępnienie przekraczałoby możliwości finansowe lub techniczne podmiotu zobowiązanego. W takim przypadku dane te należy jednak udostępnić później, ale z uwzględnieniem ich wartości (potencjału) gospodarczej i społecznej, a więc w takim terminie, aby możliwe byłoby ich wykorzystanie.

Na wstępie wspomnieliśmy także, czym są dane wysokiej wartości. Ustawa również i w ich przypadku przewiduje szczególne zasady udostępniania. Są one udostępniane bezpłatnie, poprzez API oraz zbiorczo, o ile to możliwe. Ciekawe jest jednak to, że zasadniczo powinny być one w formacie nadającym się do odczytu maszynowego, czyli – bazując na definicji ustawowej – w formacie pliku ustrukturyzowanym tak, aby programy komputerowe mogły łatwo zidentyfikować, rozpoznać i pozyskać określone dane i ich wewnętrzną strukturę bez utraty ich semantycznej interoperacyjności. Innymi słowy – łatwym do odczytu przez algorytm. Warto nadmienić, że w odniesieniu do pewnych kategorii danych wysokiej wartości (m.in. dane geoprzestrzenne) wymagania będą doprecyzowane w drodze rozporządzeń właściwych ministrów.

Wniosek o ponowne wykorzystanie danych

To bardzo istotny element Ustawy, która przewiduje konkretne sytuacje, kiedy dane udostępnia się właśnie w tym trybie. Są to następujące przypadki:

1. informacje sektora publicznego nie zostały udostępnione w BIP lub na portalu danych,
2. informacja została udostępniona w innym systemie niż BIP czy portal danych i nie zostały określone warunki dodatkowe lub opłaty lub nie ma takiej informacji o warunkach lub opłatach,
3. informacja będzie wykorzystana na innych warunkach niż przewiduje to Ustawa lub podmiot udostępniający,
4. informacja została udostępniona lub przekazana na podstawie innej ustawy.

Sam wniosek nie musi dotyczyć wyłącznie jednostkowej informacji, ale może obejmować umożliwienie udostępniania w sposób stały i bezpośredni, w czasie rzeczywistym, określonych informacji. W Ustawie przewidziano minimalny zakres informacji, które powinny znaleźć się w takim wniosku, choć można założyć, że podmioty zobowiązane będą publikowały własne wzorce. We wniosku należy więc wskazać przede wszystkim:

1. nazwę podmiotu zobowiązanego;
2. podstawowe informacje o wnioskodawcy (identyfikacyjne, w tym imię i nazwisko oraz adres – nowe możliwości pojawią się także wraz ze wdrażaniem ustawy o doręczeniach elektronicznych);
3. konkretną informację oraz – jeżeli dotyczy tej kategorii – warunki wykorzystania, źródło udostępnienia lub przekazania;
4. cel ponownego wykorzystania, w tym poprzez określenie rodzaju działalności, w której informacje

sektora publicznego będą ponownie wykorzystywane – tutaj Ustawa nakazuje przywołanie konkretnych dóbr, produktów lub usług, jednak założyć można, że zasadnym będzie dołączenie informacji o PKD;
5. wskazanie formy przygotowania informacji lub wskazanie formatu danych;
6. wskazanie sposobu przekazania informacji.

Ustawa nakazuje również, aby we wniosku znalazła się informacja odnośnie do okresu, przez który podmiot zobowiązany będzie umożliwiał wykorzystanie informacji sektora w sposób stały i bezpośredni w czasie rzeczywistym, o ile tego dotyczył też wniosek. Sam wniosek będzie można złożyć zarówno w postaci papierowej, jak i elektronicznej, w tym – jak można założyć – z użyciem profilu zaufanego i kwalifikowanego podpisu elektronicznego.

Po przekazaniu wniosku może okazać się, że nie spełnia on warunków formalnych, np. nie zawiera wszystkich fakultatywnych danych. W takiej sytuacji podmiot zobowiązany ma obowiązek wezwać wnioskodawcę do jego uzupełnienia wraz z pouczeniem, że w przypadku nieprzekazania uzupełnionego wniosku w terminie 7 dni od dnia otrzymania wezwania, spowoduje to pozostawienie wniosku bez rozpoznania.

Jeżeli jednak wniosek jest poprawny, to podmiot rozpatrzy wniosek niezwłocznie, ale nie później niż w terminie 14 dni od dnia otrzymania dokumentu. Jest to zasada, od której jednak przewidziano wyjątek. Jeżeli z jakichś względów rozpoznanie nie może nastąpić w tym 14-dniowym terminie, to podmiot ma obowiązek poinformować wnioskodawcę o opóźnieniu i jego przyczynach oraz wskazać termin rozpatrzenia wniosku nie dłuższy niż 2 miesiące.

Po rozpatrzeniu wniosku podmiot zobowiązany ma kilka opcji. Może po pierwsze przekazać informację bez wskazywania warunków (to opcja najbardziej korzystna dla wnioskodawcy). Może także:
1. poinformować o braku informacji,
2. poinformować o braku warunków wykorzystywania, jeżeli wnioskodawca ma już informacje,

3. złożyć ofertę (lub poinformować o wysokości opłat) – tutaj dopuszczalny jest sprzeciw lub zawiadomienie o przyjęciu (mamy też milczącą zgodę po 14 dniach) lub
4. odmówić – w drodze decyzji – wyrażenia zgody na ponowne wykorzystanie.

Pytanie, kiedy podmiot może odmówić udostępnienia informacji. Może to nastąpić w przypadkach określonych w art. 6, które już sobie omówiliśmy (m.in. tajemnica handlowa bez zgody czy ograniczenia wynikające z przepisów o ochronie informacji niejawnych). Ramy opracowania nie pozwalają na szczegółowe omówienie procedury odwoławczej, ale istotne jest to, że odwołanie od decyzji przysługuje do ministra właściwego do spraw informatyzacji.

Koszty

Zasadą, określoną zarówno w Ustawie, jak i *Data Governance Act*, jest udostępnianie lub przekazywanie danych w celu ponownego wykorzystania bezpłatnie, ale jak to zwykle bywa jest też ale. Jeżeli przygotowanie lub przekazanie informacji w sposób lub w formie wskazanych we wniosku o informacji wymaga poniesienia dodatkowych kosztów, to podmiot może nałożyć na wnioskodawcę dodatkową opłatę.

Taka opłata nie może być jednak dowolnie określona. Ustawa wyraźnie wskazuje, że przy jej ustalaniu należy wziąć pod uwagę koszty przygotowania lub przekazania oraz inne czynniki, które mogą wpłynąć na wygenerowanie nowych kosztów. Opłata nie może jednak przekroczyć rzeczywiście poniesionych kosztów. Ważne jest przy tym to, że określając wysokość opłaty, podmiot może uwzględnić koszty anonimizacji danych osobowych wraz ze środkami zastosowanymi w celu ochrony tajemnicy przedsiębiorstwa. W przypadku danych przekazywanych w sposób stały i bezpośredni w czasie rzeczywistym, dodatkowa opłata może pojawić się w związku z koniecznością dostosowania systemu IT itd.

Na koniec warto wskazać, że na żądanie wnioskodawcy podmiot zobowiązany ma obowiązek wskazać sposób obliczenia takiej opłaty.

Michał Nowakowski
doktor nauk prawnych i radca prawny; założyciel bloga www.finregtech.pl i prawnik w jednej z instytucji finansowych; pasjonat nowych technologii, członek Grupy Roboczej ds. sztucznej inteligencji przy KPRM oraz członek Komisji LegalTech przy Okręgowej Izbie Radców Prawnych w Warszawie, autor książki pt. „Fintech – regulacje, finanse, technologie. Praktyczny przewodnik dla sektora innowacji finansowych"

1 https://eur-lex.europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:52020DC0066&from=PL
2 Dz. Urz. UE z 2019 r., L-172/56.
3 Pełen katalog nie został tutaj wskazany ze względu na ograniczone ramy opracowania.
4 Dz.U. 2005 nr 64 poz. 565.

Nowa ustawa – Prawo komunikacji elektronicznej

Obowiązki dostawców usług komunikacji interpersonalnej niewykorzystujących numerów

Michał Czuryło

Potrzeba dokonania zmian w przepisach prawa polskiego w obszarze komunikacji elektronicznej wynika z przyjęcia dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. *ustanawiająca Europejski kodeks łączności elektronicznej*[1] (dalej zwanej „Dyrektywą").

Nowa Dyrektywa

Przed przyjęciem Dyrektywy funkcjonowało pięć różnych innych dyrektyw, które łącznie stanowiły obowiązujące ramy regulacyjne dla sieci i usług łączności elektronicznej. Przeciwdziałanie fragmentacji regulacyjnej występującej na rynku telekomunikacyjnym było jednym z celów, które nakreśliła Komisja Europejska w komunikacie z dnia 6 maja 2015 r. ustanawiającym strategię jednolitego rynku cyfrowego dla Europy[2]. Miało to sprzyjać bardziej spójnemu stosowaniu przepisów oraz większej skuteczności regulacji, a co za tym idzie – polepszeniu ochrony konsumentów czy zrównaniu warunków działania wszystkich uczestników rynku. Równie istotnym celem było dostosowanie przepisów do nowych realiów rynkowych.

Dyrektywa rozróżnia usługi łączności interpersonalnej wykorzystujące i niewykorzystujące numery. Te pierwsze opierają swoje funkcjonowanie o przydzielone użytkownikom końcowym numery identyfikacyjne. Te drugie nie wymagają wykorzystania takich numerów dla nawiązania łączności – nie korzystają z publicznie nadanych zasobów numeracyjnych pochodzących z krajowych lub międzynarodowych planów numeracji, ani nie umożliwiają połączenia z takimi numerami i w związku z tym nie uczestniczą w gwarantowanym przez władze publiczne interoperacyjnym środowisku. Odmienne traktowanie usług łączności interpersonalnej wykorzystujących numery jest uzasadnione, ponieważ są one uczestnikami zagwarantowanego przez organy publiczne interoperacyjnego środowiska, a zatem również z niego korzystają.

Unijny prawodawca zauważył jednak rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów i w związku z tym stwierdził, że usługi te również powinny podlegać odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem. Poziom bezpieczeństwa powinien odpowiadać przy tym istniejącemu ryzyku związanemu z korzystaniem z tych usług. W Dyrektywie stwierdzono, że poziom ryzyka w przypadku usług niewykorzystujących numerów jest niższy, ponieważ dostawcy tych usług, w przeciwieństwie do tradycyjnych usług łączności elektronicznej, nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach.

W Dyrektywie przewidziano również, że zgodnie z zasadą proporcjonalności szereg przepisów dotyczących praw użytkowników końcowych, nie powinien mieć zastosowania do mikroprzedsiębiorstw, które dostarczają usługi łączności interpersonalnej niewykorzystujące numerów. Usług łączności interpersonalnej niewykorzystującej numerów nie powinny też dotyczyć ograniczenia w możliwości dokonywania zmian warunków umownych przez dostawców publicznie dostępnych usług łączności. W stosunku do takich dostawców przewidziano ogólnie, że dokonywane przez nich zmiany warunków umownych, które nie są korzystne (albo gdy połączono zmiany korzystne z niekorzystnymi) dla użytkownika końcowego, powinny dawać użytkownikowi prawo do rozwiązania umowy bez ponoszenia kosztów.

Dyrektywa przewidziała, że jej transpozycja, czyli wprowadzenie jej postanowień do prawa krajowego, powinna nastąpić w terminie najpóźniej do dnia 21 grudnia 2020 r. W tym czasie powinny powstać i zostać przyjęte i opublikowane przepisy niezbędne do wykonania Dyrektywy.

Transpozycja i data wejścia w życie PKE

Projekt ustawy – Prawo komunikacji elektronicznej[3] (dalej „Projekt PKE") został sporządzony przez Ministerstwo Cyfryzacji i nosi datę 29 lipca 2020 r. Projektowana ustawa ma zastąpić aktualnie obowiązującą ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[4] (dalej PT). Prawie siedemnaście lat, które minęły od uchwalenia PT, to w przypadku rozwoju technologii cała epoka. Również autorzy projektu podkreślają dynamicznie postępujący proces informatyzacji gospodarki będący następstwem rozwoju technologii informacyjno-komunikacyjnych. Technologie mają duży wpływ na przemiany w obszarze komunikacji międzyludzkiej, a co za tym idzie – na wszelkie obszary życia i biznesu, gdzie ta komunikacja ma istotne znaczenie. Za wprowadzeniem nowej regulacji przemawiać ma również zakres i liczba zmian, które nastąpiły w przepisach we wspomnianym siedemnastoletnim okresie, co powoduje konieczność uporządkowania przepisów z zakresu prawa telekomunikacyjnego.

W momencie publikacji niniejszego artykułu został już przekroczony określony w Dyrektywie termin jej transpozycji. Z przepisów opublikowanego 12 lutego 2021 r. projektu ustawy – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej[5] wynika, że przewiduje się wejście w życie PKE po upływie

sześciu miesięcy od dnia jej ogłoszenia. Twórcy przepisów zakładali, że PKE wejdzie w życie na początku 2021 r., co jednak okazało się nierealne.

Oprócz regulacji, których wdrożenia do polskiego porządku prawnego wymaga Dyrektywa, Projekt PKE zawiera również zestaw przepisów w zakresie zasad przetwarzania danych telekomunikacyjnych oraz ochrony tajemnicy komunikacji elektronicznej stanowiącej wdrożenie dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[6] oraz kwestie wymagań dla urządzeń radiowych, które wdrażają przepisy dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylającej dyrektywę 1999/5/WE[7]. Przepisy te nie zostały w prosty sposób przeniesione do Projektu PKE – ich treść wymagała uwzględnienia brzmienia przepisów Dyrektywy i w związku z tym pewnego doprecyzowania. Tajemnicą telekomunikacyjną objęto więc także dostawców usług komunikacji interpersonalnej niewykorzystującej numeracji, a także podmioty z nimi współpracujące. Również przetwarzanie danych osobowych niezbędnych do świadczenia usług komunikacji elektronicznej przez dostawców usług komunikacji interpersonalnej niewykorzystujących numerów znalazło swoje uregulowanie w przepisach Projektu PKE.

Objęcie usług komunikacji interpersonalnej niewykorzystującej numerów przepisami Projektu PKE

Jednym z zagadnień, które do tej pory nie doczekało się uregulowania w PT i jest w związku z tym swoistym *novum* w polskim prawie, są zasady dotyczące dostawców publicznie dostępnych usług komunikacji interpersonalnej niewykorzystującej numerów. Nowe przepisy mają w założeniu zwiększyć prawa użytkowników końcowych korzystających z tych usług.

Świadczenie usług komunikacji interpersonalnej niewykorzystujących numerów zostało jednoznacznie uznane za działalność polegającą na zapewnieniu komunikacji elektronicznej i objęte regulacją PKE prócz „tradycyjnej" działalności telekomunikacyjnej, czyli świadczenia usług telekomunikacyjnej, dostarczania sieci telekomunikacyjnych i świadczenia usług z tym powiązanych. Przedsiębiorcy świadczący takie usługi zaliczeni zostają natomiast do kategorii dostawców usług komunikacji elektronicznej.

Co to oznacza?

Próbując ustalić, co mieści się w zakresie nowej kategorii usług, zacząć należy od stwierdzenia, że usługi te muszą spełniać wymogi stawiane dla usług komunikacji interpersonalnej, czyli:

1) umożliwiać bezpośrednią interpersonalną – tzn. między osobami fizycznymi, również jeżeli osoby te działają w imieniu osób prawnych czy innych jednostek organizacyjnych i interaktywną, to znaczy pozwalającą na udzielanie odpowiedzi – wymianę informacji;
2) za pośrednictwem sieci telekomunikacyjnej;
3) między skończoną liczbą osób (czyli w założeniu niekierowaną do potencjalnie nieograniczonej liczby odbiorców);
4) gdzie osoby inicjujące połączenie lub w nim uczestniczące decydują o jego odbiorcy lub odbiorcach.

Jako przykłady takich usług podaje się połączenia głosowe, jak również pocztę elektroniczną, usługi przekazywania wiadomości lub czaty grupowe. Usługami, które zdobywają coraz większy udział w rynku i będą mieścić się w definicji usług komunikacji interpersonalnej, będą w szczególności komunikatory internetowe. Z drugiej strony usługami, które **nie będą** mieścić się w podanych ramach, będą strony internetowe, serwisy społecznościowe czy blogi, a także na przykład usługa dostarczania wideo na żądanie.

Z tej definicji jednocześnie zostały wyłączone te z usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej. Wskazówkę, jak rozumieć to wyłączenie, znajdziemy w motywach do Dyrektywy, gdzie podane jest, że chodzi o takie usługi, które stanowią wyłącznie nieznaczny dodatek do innej usługi i z obiektywnych przyczyn taki dodatek nie może być użytkowany bez usługi głównej. Integracja tego dodatku z usługą główną nie może też służyć obejściu wymogów, jakie stawiają przepisy wobec usługi komunikacji interpersonalnej. Dobrym przykładem jest tu możliwość komunikowania się między graczami w rozgrywkach typu multiplayer, która służy jedynie jako dodatek do samej rozgrywki będącej usługą podstawową i może tę rozgrywkę ułatwiać, choć wcale nie musi być dla jej prowadzenia niezbędna.

Te z usług komunikacji interpersonalnej, które nie umożliwiają realizacji

połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji, będą właśnie usługami komunikacji interpersonalnej niewykorzystującej numerów. Z drugiej strony PKE wyraźnie określa, że usługi komunikacji interpersonalnej niewykorzystującej numerów wyłączone zostają z definicji usługi telekomunikacyjnej. Do usług telekomunikacyjnych zaliczać będą się więc usługi komunikacji interpersonalnej wykorzystujące numery. Zatem dostawca usług komunikacji interpersonalnej niewykorzystującej numerów nie będzie jednocześnie dostawcą usług telekomunikacyjnych.

Obowiązki przedsiębiorców świadczących nowo zdefiniowany rodzaj usług

Na dostawców usług komunikacji elektronicznej nałożono w Projekcie PKE szereg nowych obowiązków, wśród których należy wskazać:

1) obowiązek odpowiadania na zapytania Prezesa Urzędu Komunikacji Elektronicznej (dalej „Prezesa UKE") na równi z przedsiębiorcami telekomunikacyjnymi,
2) obowiązki dotyczące obronności i bezpieczeństwa państwa,
3) uprawnienie Prezesa UKE do nakładania obowiązków regulacyjnych,
4) obowiązki informacyjne wobec użytkowników końcowych.

Z racji tego, że dostawców usług komunikacji interpersonalnej niewykorzystującej numerów (dalej „Dostawcy") objęto Projektem PKE, w stosunku do nich zacznie obowiązywać szereg wymagań, jakie częściowo do tej pory obejmowały inne podmioty na gruncie PT. Z jednej strony duża część obowiązków wynikających z Projektu PKE nie stosuje się do przedsiębiorców komunikacji elektronicznej świadczących wyłącznie publicznie dostępne usługi komunikacji interpersonalnej niewykorzystujące numerów będących mikroprzedsiębiorcami.

Z drugiej, Prezes UKE, w drodze decyzji, może nałożyć na podmiot świadczący usługi komunikacji interpersonalnej niewykorzystującej numerów, które osiągnęły znaczny poziom zasięgu i upowszechnienia wśród użytkowników, dodatkowo obowiązki w zakresie:

1) zapewnienia dostępu do interfejsu programistycznego aplikacji oraz
2) zapewnienia związanych z tymi usługami udogodnień, które służą zapewnieniu możliwości zapoznania się z treścią przez osoby z niepełnosprawnościami.

Prezes UKE może nałożyć te obowiązki wyłącznie w sytuacji, gdy możliwość komunikowania się między użytkownikami końcowymi jest zagrożona ze względu na brak interoperacyjności między usługami komunikacji interpersonalnej oraz takie zagrożenie zostało stwierdzone przez Komisję Europejską.

Istotna grupa obowiązków, które Projekt PKE nakłada na dostawców, dotyczy bezpieczeństwa świadczonych usług. Dostawca, w celu zapewnienia ciągłości działania świadczonych usług, jest zobowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia, czyli stanów nadzwyczajnych, sytuacji kryzysowych w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym lub bezpośredniego zagrożenia dla bezpieczeństwa sieci i usług[8]. Obowiązki w zakresie bezpieczeństwa obejmują w szczególności konieczność przeprowadzania systematycznej oceny ryzyka wystąpienia zagrożenia, podejmowania środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do poziomu ryzyka oraz dokumentowania podejmowanych działań. Nietrudno zauważyć, że zarówno zakres, jak i sposób opisania tych obowiązków przypomina treść obowiązków administratorów danych osobowych, jakie wynikają chociażby z przepisów rozporządzenia 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)[9] (RODO). Zasadne są więc uwagi w zakresie „neutralności technologicznej" nowych przepisów – ustawodawca nie proponuje konkretnych rodzajów zabezpieczeń, ale kładzie nacisk na ich adekwatność, którą

można zapewnić tylko wtedy, jeżeli ich wprowadzenie poprzedzone zostanie oceną ryzyka. Niezbędnym krokiem zabezpieczającym interesy prawne każdego Dostawcy jest w związku z tym odpowiednie dokumentowanie podejmowanych działań, co pozwalać będzie w przyszłości wykazać rzeczoną adekwatność, chociażby w przypadku podejmowania działań kontrolnych przez odpowiedni organ.

Kolejnym istotnym obowiązkiem w zakresu bezpieczeństwa, również przywodzącym na myśl ten wynikający z RODO, jest konieczność informowania Prezesa UKE o wystąpieniu incydentu bezpieczeństwa oraz o podjętych działaniach zapobiegawczych i środkach naprawczych. Definicja incydentu bezpieczeństwa jest dosyć szeroka – jest to każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług. Poinformowanie powinno nastąpić w bardzo krótkim, 24-godzinnym terminie, liczonym od wykrycia incydentu. Tu jednak widzimy różnicę w stosunku do obowiązku notyfikacji wynikającego z RODO, zgodnie z którym termin liczony jest **od stwierdzenia naruszenia ochrony danych osobowych**, a w ramach „stwierdzenia" Europejska Rada Ochrony Danych przewiduje czas na dokonanie oceny, czy rzeczywiście do naruszenia doszło. Skrócenie terminu do 24 godzin oraz posłużenie się pojęciem „wykrycia" w Projekcie PKE zdaje się być bardziej rygorystyczne niż i tak uznawane za surowe obowiązki notyfikacji wynikające z RODO. Co istotne progi incydentu bezpieczeństwa, których

spełnienie spowoduje powstanie obowiązku informacyjnego, mają zostać określone w rozporządzeniu ministra właściwego do spraw informatyzacji, co też jest rozwiązaniem odmiennym niż zastosowane w RODO. Dostawca, który wykonuje działalność na rynku detalicznym, ma być obowiązany do zamieszczania informacji na swojej stronie internetowej o wystąpieniu incydentu i jego wpływie na dostępność świadczonych usług, jeżeli wpływ ten jest istotny.

W Projekcie PKE uregulowano również uprawnienia Prezesa UKE do dokonywania oceny podjętych przez Dostawcę środków zapewniających bezpieczeństwo sieci i usług. Dostawca musi informować o podjętych środkach, celem umożliwienia Prezesowi UKE realizacji jego uprawnienia, a Prezes UKE, po dokonaniu powyższej oceny, może w drodze decyzji nałożyć na Dostawcę obowiązek zastosowania dodatkowych środków zapewniających bezpieczeństwo sieci lub usług albo poddania się audytowi, którego wyniki przedsiębiorca udostępnia Prezesowi UKE.

Na Dostawcę w Projekcie PKE zostały również nałożone obowiązki związane z przetwarzaniem danych osobowych. Zdają się one w pewnym zakresie pokrywać z obowiązkami, które już wynikają z przepisów RODO, choć nie w całości. Przepisy Projektu PKE wymagają chociażby wdrożenia polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych, podczas gdy RODO nie przewiduje wprost konieczności posiadania takiego dokumentu, wskazując tylko, że jednym ze środków wymaganych od administratorów jest wdrożenie odpowiednich polityk ochrony danych, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania. W Projekcie PKE przewidziano również wyraźny obowiązek prowadzenia rejestru naruszeń danych osobowych z określeniem, co w tym rejestrze ma się znajdować. Ponownie jest to wymóg bardziej szczegółowy niż wynikający z RODO, gdzie jedynie określono, iż administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, nie wskazując konkretnie, że dokumentowanie ma przyjąć formę rejestru o określonej zawartości.

Sankcje za naruszenie przepisów Projektu PKE

Zwracać musi uwagę bardzo obszerny i określony w dosyć kazuistyczny sposób katalog przypadków, za które w Projekcie PKE przewidziano sankcję w postaci kary pieniężnej. Część z tych przypadków wyraźnie dotyczy Dostawców; np. kary pieniężne nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Osobne zasady obliczania kary określono dla podmiotów, które nie przekroczyły wskazanych w przepisach progów w zakresie przychodu w poprzednim roku kalendarzowym lub które nie przekażą informacji o wysokości osiągniętego przychodu. Co istotne decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności. Ustalając wysokość kary pieniężnej, Prezes UKE uwzględnia charakter i zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe.

Niezależnie od kar pieniężnych Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia. Ponieważ usługi komunikacji interpersonalnej niewykorzystującej numerów nie mieszczą się w definicji usług telekomunikacyjnych, to w przypadku osób zarządzających przedsiębiorstwami dostarczającymi ten szczególny rodzaj usług ta dodatkowa odpowiedzialność nie będzie mogła być nałożona.

Podsumowanie

Wejście w życie przepisów Projektu PKE oznacza powstanie szeregu nowych obowiązków dla podmiotów dostarczających usługi komunikacji interpersonalnej niewykorzystującej numerów. Są to obowiązki nowe i z pewnością stanowić będą wyzwanie dla co najmniej części z tych przedsiębiorców, do którego to obowiązku należy zacząć przygotowywać się odpowiednio wcześniej. Jak dodatkowo przewidują autorzy Projektu PKE, wejście w życie jego przepisów, w tym również właśnie objęcie tymi przepisami przedsiębiorców świadczących usługi komunikacji interpersonalnej niewykorzystującej numerów, spowoduje istotne konsekwencje również dla budżetu, w tym wynikające z potrzeby zwiększenia zatrudnienia w urzędach centralnych (UKE oraz w wybranych ministerstwach), a także z potrzeby wydania poradnika dla przedsiębiorców z zakresu nowych regulacji.

Michał Czuryło
radca prawny, wpisany na listę w OIRP w Krakowie od 2013 r., absolwent studiów prawniczych na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego oraz Szkoły Prawa Amerykańskiego współorganizowanej przez Columbus School of Law The Catholic University w Waszyngtonie, Certified Information Privacy Professional – Europe (CIPP/E), specjalizuje się w ochronie danych, prawie nowych technologii, prawie własności intelektualnej, a także w procedurze administracyjnej, partner w Konieczny, Wierzbicki Kancelaria Radców Prawnych, specjalizującej się w dziedzinie szeroko rozumianego prawa gospodarczego, nowych technologii, korporacyjnego, budowlanego oraz prawa cywilnego

1 Dziennik Urzędowy Unii Europejskiej L 321 z 17 grudnia 2018 r., s. 36.
2 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Strategia jednolitego rynku cyfrowego dla Europy z dnia 6 maja 2015 r. COM(2015) 192 final.
3 Projekt opublikowany w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji pod numerem UC45, https://legislacja.gov.pl/projekt/12336501 – dostęp z 13 kwietnia 2021 r., godzina 17:36.
4 Tekst jednolity: Dziennik Ustaw z 2021 r., poz. 576.
5 Projekt opublikowany w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji pod numerem UC46, https://legislacja.gov.pl/projekt/12336502 – dostęp z 13 kwietnia 2021 r., godzina 17:37.
6 Dziennik Urzędowy Wspólnot Europejskich L 201 z 31 lipca 2002 r., s. 37.
7 Dziennik Urzędowy Unii Europejskiej L 153 z 22 maja 2014 r., s. 62.
8 Tekst jednolity: Dziennik Ustaw z 2020 r., poz. 1856 wraz z późniejszymi zmianami.
9 Dziennik Urzędowy Unii Europejskiej L 119 z 4 maja 2016 r., s. 1.

Marketing e-mailowy

Jak prowadzić go w firmie legalnie, aby ciągle był skuteczny?

Ilona Przetacznik

Marketing i sprzedaż to zazwyczaj dwa najważniejsze elementy w każdej firmie. Przedsiębiorcy wiedzą, że bez skutecznego marketingu nie będzie skutecznej sprzedaży. Do tego wszystkiego dochodzą przepisy prawa, które często zaburzają konwersję lub znacznie ją obniżają. Jednak czy zawsze? Czy marketing mailowy w małej firmie może być jednocześnie skuteczny i zgodny z przepisami prawa, w szczególności z owianym złą sławą RODO? Może! Wystarczy pamiętać o kilku podstawowych zasadach i obowiązkach prawnych.

E-mail marketing jako najskuteczniejszy sposób sprzedaży

E-mail marketing to ciągle jeden z najskuteczniejszych sposobów sprzedażowych. Nawet jeśli są osoby, które twierdzą, że należy skupić się jedynie na działaniu w mediach społecznościowych, typu Facebook, Instagram czy YouTube, to dobrzy specjaliści od marketingu mailowego potrafią zarobić setki tysięcy złotych na odpowiednich lejkach sprzedażowych zawierających kilka wiadomości e-mail.

Należy bowiem pamiętać, że media społecznościowe to nie jest narzędzie należące do jakiegokolwiek przedsiębiorcy. Jest to teren właściciela danego portalu, który w każdej chwili może ten portal usunąć. I nawet jeśli jest to rozważanie czysto teoretyczne, to jednak zawsze istnieje takie niebezpieczeństwo.

Inaczej jest z adresami e-mail, które – jeśli są prawidłowo zbierane i przechowywane – mogą stanowić bazę marketingową firmy na bardzo długi czas.

To właśnie dlatego należy zacząć od podstaw prawnych prawidłowego budowania bazy mailowej.

W pierwszej kolejności należy zastanowić się, w jaki sposób będą gromadzone e-maile.

Do sposobów tych należą m.in.:

- tworzenie własnej bazy danych zebranych e-maili w pliku wewnętrznym typu Excel,
- korzystanie z narzędzia CRM do zarządzania kontaktem mailowym z klientami,
- zapisywanie danych w chmurze, np. GSuite czy Dropbox, w różnych formatach,
- agregowanie danych w skrzynce mailowej, np. Gmail, Outlook,
- korzystanie z zewnętrznych dostawców systemów do e-mail marketingu (Email Service Provider), np. MailerLite, Freshmail, GetResponse czy Active Campaign.

Korzystając ze wskazanych narzędzi, należy pamiętać o obowiązkach prawnych, a przede wszystkim o:

- zawarciu umowy powierzenia przetwarzania danych osobowych z dostawcami narzędzi do e-mail marketingu czy dostawcami CRM-ów; jeśli przedsiębiorca powierza im swoje dane, aby korzystać z funkcjonalności danego narzędzia, a adresy e-mail należą do przedsiębiorcy, to wówczas taka umowa jest obowiązkiem;
- zawarciu umów powierzenia także z podmiotami, które obsługują bazę danych, czyli np. ze współpracownikami, wirtualną asystentką albo agencją marketingową;
- umieszczeniu w klauzuli informacyjnej związanej z ochroną danych osobowych informacji na temat odbiorców danych, czyli podmiotach trzecich, którym dane są powierzane.

Sposoby poszukiwania e-maili do bazy

Na różne sposoby można także poszukiwać potencjalnych klientów, a tym samym ich adresy e-mail. Dzieje się to m.in. poprzez:

- tworzenie własnej bazy danych zebranych e-maili ze źródeł powszechnie dostępnych, np. CEIDG, KRS, na stronach agregujących dane adresowe firm czy stronach-wizytówkach firm;
- tworzenie bazy e-maili dotychczasowych klientów, którzy już skorzystali z usług lub kupili jakiś produkt;
- zbieranie bazy danych na podstawie poleceń dotychczasowych klientów lub znajomych;
- dodawanie do bazy e-maili, które zostały podane przez osoby zainteresowane wysłaniem im oferty handlowej.

Do oceny, czy powyżej wskazane sposoby na zarządzanie adresami e-mail i budowanie bazy mailingowej są legalne, istotne jest określenie procesów występujących w firmie i ich poszczególnych etapów.

Budując bazę mailingową, trzeba pamiętać o spełnieniu obowiązków prawnych na każdym etapie. Od momentu wykorzystania narzędzi do budowania bazy mailingowej i zawarcia wspomnianych już umów powierzenia przetwarzania danych osobowych po wysłanie odpowiedniej treści obowiązku

informacyjnego, uzyskanie zgód i realizację zasady rozliczalności. Każdorazowo należy mieć odpowiednią podstawę prawną przetwarzania danych osobowych, które gromadzi firma. Adresy e-mail zazwyczaj należą do kategorii danych osobowych, ale nie zawsze.

Kiedy adres e-mail jest, a kiedy nie jest daną osobową?

Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, której dane dotyczą. Jak precyzuje dalej art. 4 pkt 1 Rozporządzenia 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 jako RODO) możliwa do zidentyfikowania osoba fizyczna to taka, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię, nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Aby uznać konkretny adres e-mail za dane osobowe, należy mieć pewność albo chociaż uzasadnione przypuszczenie, że należy on do konkretnej osoby lub że taką osobę można zidentyfikować na podstawie takiego adresu e-mail.

Logiczne jest twierdzenie, że jeśli e-mail nie zawiera w swojej nazwie imienia i nazwiska, to ciężko będzie zidentyfikować taką osobę. To jednak może być ryzykowne i każdy przypadek należy rozpatrywać indywidualnie.

Przykład

E-mail o nazwie biuro@firma.pl nie wskazuje na dane osobowe. Jednak e-mail biuro@adamkowalski.pl już tak, nawet jeśli obsługuje go pracownik biurowy. Podobnie rzecz się ma z e-mailami, które pośrednio mogą wskazywać na dane osobowe, np. kontakt@akowalski.pl, hello@annan.com. Dotyczy to także stanowisk czy funkcji i możliwości powiązania ich z konkretną osobą, np. jedyna w firmie funkcja inspektora ochrony danych osobowych i jego adres iod@firma.pl albo funkcja PR-owca: pr@firma.pl. Dotyczy to w szczególności pracowników danej firmy[1].

W swoje bazie danych należy albo wyselekcjonować adresy e-mail, które wyraźnie wskazują na dane osobowe i zawsze dbać o uzyskanie odpowiednich zgód marketingowych, albo też wszystkie adresy e-mail traktować jako dane osobowe i zawsze stosować tę samą procedurę odebrania zgód i przekazania obowiązku informacyjnego. Druga opcja jest stosowana wówczas, gdy tych adresów jest bardzo dużo i praca nad selekcją bazy byłaby mniej efektywna niż stworzenie jednego powtarzalnego procesu, w tym także procesu realizacji żądań osób, których dane dotyczą.

Czy uzyskanie zgody na marketing e-mailowy jest zawsze wymagane przez RODO?

RODO nie wymaga zgody na marketing bezpośredni. W motywie 47 Preambuły RODO *in fine* wprost pozwala na kierowanie marketingu bezpośredniego własnych produktów i usług na podstawie tzw. prawnie uzasadnionego interesu administratora, o którym mowa w art. 6 ust. 1 lit. f) RODO.

Warunkiem dopuszczalności przetwarzania danych osobowych na tej podstawie jest przeprowadzenie testu równowagi i uznanie, że interes administratora danych w przetwarzaniu danych osobowych jest co najmniej równoważny wobec praw, wolności i interesów podmiotów danych osobowych[2]. Wykonany test należy dołączyć do swojej dokumentacji RODO w firmie.

Należy jednak pamiętać, że RODO to nie jedyny akt prawny, który trzeba mieć na uwadze w kontekście usług marketingowych i wysyłania ofert handlowych.
Przepisy szczególne w polskim porządku prawnym zawierają bardziej rygorystyczne warunki.

Art. 10 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344, dalej UŚUDE) uzależnia możliwość wysyłania informacji handlowych za pomocą środków komunikacji elektronicznej od zgody adresata informacji, będącego osobą fizyczną.

Z kolei, art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2021 r. poz. 576, dalej jako PT) zakazuje używania telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, dopuszczając ich zastosowanie jedynie na podstawie zgody abonenta lub użytkownika końcowego.

Kiedy należy uzyskać zgodę na wysyłkę oferty e-mailem?

Zgodnie ze wspomnianym już art. 10 ust. 1 UŚUDE prowadzenie marketingu bezpośredniego poprzez wysyłkę wiadomości e-mail wymaga zgody odbiorcy, będącego osobą fizyczną tylko w sytuacji wysyłania informacji przez niego niezamówionych.

Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji. Może to stać się także poprzez udostępnienie w tym celu identyfikującego go adresu elektronicznego[3].

Wysyłka ofert niezgodnie ze wspomnianym przepisem stanowi czyn nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2018 r. poz. 419 z późn. zm., dalej ZNK), na co wskazuje art. 10 ust. 3 UŚUDE.

Marketing e-mailowy, co do zasady, wymaga zatem uzyskania odpowiednich zgód na wysyłkę ofert handlowych, zanim ta oferta zostanie wysłana

do oznaczonej osoby fizycznej. Dotyczy to głównie sytuacji, gdy w adresie e-mail przetwarzane są dane osobowe.

A kiedy nie trzeba uzyskiwać zgody na wysyłkę mailingu? Dzieje się tak w sytuacji:

- gdy adres e-mail nie wskazuje na dane osobowe,
- gdy należy do osoby prawnej, a nie fizycznej (z zastrzeżeniem, o którym dalej),
- gdy osoba „zamówiła", czyli poprosiła o ofertę, zadała pytanie dotyczące danego produktu lub usługi i zostały mu one wysłane zgodnie z zapytaniem,
- gdy osoba pyta o zgodę na wysyłkę oferty.

Jak uzyskać prawidłową zgodę na wysyłkę oferty?

Zgoda, aby była prawidłowa, powinna mieć określone cechy. Są one wskazane przez RODO i pozostałe przepisy prawa.

W art. 4 pkt 11 RODO wskazuje, że „zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych".

Zgoda powinna być dobrowolna, konkretna, świadoma, jednoznaczna, rozliczalna i łatwa do wycofania[4].

Zakazane są zgody milczące, zaznaczone z góry, ukryte w innych dokumentach, np. w regulaminie.

Jeżeli przedsiębiorca nie posiada zgód odpowiadających wymogom RODO, polskiej ustawie o ochronie danych osobowych oraz UŚUDE, to będzie musiał je uzyskać, aby zalegalizować swoją dotychczasową bazę mailingową.

Można to zrobić poprzez ponowne skierowanie prośby o wyrażenie zgody do właścicieli e-maili wraz z jednoczesnym przesłaniem do nich obowiązku informacyjnego. Proces można zautomatyzować poprzez zastosowanie strony lądowania (tzw. landing page) i odpowiednich checkboxów niezbędnych do zaznaczenia, aby na przykład uzyskać bezpłatny materiał do pobrania (np. poradnik, checklistę – tzw. lead magnet).

Jeśli chodzi o prawidłowe zbieranie zgód od nowo pozyskanych użytkowników adresów e-mail jest na to kilka sposobów.

Sposoby odebrania zgody na wysyłkę ofert handlowych na pozyskane adresy e-mail

Zgodę na wysyłkę ofert handlowych można odebrać na różne sposoby. W zależności od strategii firmy i danego procesu należy dokonać wyboru, aby zachować konwersję.

Checkbox

Zastosować checkbox, czyli okienko do zaznaczenia zgody o wskazanej treści. Bez jego zaznaczenia odbiorca nie przejdzie w procesie do kolejnego kroku. Jest to sposób znany, w szczególności jeśli chodzi o wysyłkę tzw. newsletterów. Należy pamiętać, aby checkbox nigdy nie był zaznaczony z góry, a przycisk znajdował się na samym dole (pod treścią zgody i klauzuli informacyjnej lub odesłaniem do niej).

Komunikat

Zastosować informację, z której wyraźnie wynika cel, w jakim pobierana jest zgoda odbiorcy. Powinien on być świadomy, że w momencie udostępnienia swojego adresu e-mail zostanie ten cel zrealizowany, np. zostanie mu wysłana oferta handlowa przedsiębiorstwa.

Jednoznaczna czynność potwierdzająca

O wyraźnym działaniu potwierdzającym wprost mówi RODO w art. 4 pkt 11.

Daje to możliwość szerszego pobierania zgód, w szczególności poprzez czynności dorozumiane. Złożenie oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych nie wymaga żadnej szczególnej formy[5].

Czynnością potwierdzającą może być nawet ruch telefonem w określoną stronę. Istotna jest w tym miejscu wyraźna informacja, że ten właśnie ruch wywoła udzielenie zgody na wysyłkę ofert handlowych. Może to być jednak bardzo problematyczne pod kątem rozliczalności, czyli udowodnienia uzyskania zgody odpowiadającej wymaganiom RODO i pozostałych ustaw. Jeśli jednak firma dysponuje zaawansowanymi narzędziami pozwalającymi jej na monitorowanie udzielonych zgód, a także rozliczalność, może zastosować każdy system wspierający konwersję sprzedaży.

Udostępnienie adresu poczty elektronicznej może stanowić wyrażenie zgody na otrzymywanie informacji handlowej.

Każdy z tych sposobów wymaga jednak przedstawienia obowiązku informacyjnego, co najmniej w pierwszej warstwie (tzw. warstwie podstawowej).

Przyjmuje się, że „pierwsza warstwa obowiązku informacyjnego" powinna zawierać w swej treści minimum informacje o administratorze, celach przetwarzania, prawach osoby, a także wyraźne odesłanie do pełnej treści klauzuli lub polityki prywatności[6]. Wynika to także z motywu 39 RODO. Czasami wskazuje się także na konieczność wymienienia podstawy prawnej zbierania danych i odbiorców tych danych w warstwie podstawowej[7]. Wydaje się to jednak nadmiarowe i najistotniejsze jest, aby użytkownik podający swoje dane znał tożsamość administratora, cele i wiedział, gdzie znajdzie pełną treść swoich uprawnień, kontakt do administratora i pozostałe informacje z drugiej warstwy tzw. szczegółowej.

Zasada tzw. dwóch telefonów i marketing telefoniczny

Do czynności w zakresie marketingu bezpośredniego należy także marketing telefoniczny. Marketing bezpośredni

w zakresie wykonywania telefonów jest dosyć rygorystyczny. Z jednej strony mówi się o tzw. zasadzie dwóch telefonów, a z drugiej zakazuje się nawet tego.

Zasada dwóch telefonów polega na tym, że dozwolone jest zadzwonienie do osoby w celu uzyskania zgody na prezentację oferty handlowej. Po jej otrzymaniu, w kolejnej rozmowie można przedstawić ofertę handlową.

Podstawą do pierwszego telefonu jest prawnie uzasadniony interes administratora, czyli art. 6 ust. 1 lit. f RODO. Aprobatę takiego postępowania wyraził Sąd Okręgowy Warszawa – Praga w wyroku z 4 stycznia 2019 r. o sygnaturze akt IV Ca 1873/16, który stwierdził w swym orzeczeniu, że dozwolone jest inicjowanie kontaktu telefonicznego w celu pozyskania zgody wymaganej do prowadzenia marketingu bezpośredniego z wykorzystaniem środków komunikacji elektronicznej. Sąd zwrócił uwagę na odróżnienie pojęcia marketingu bezpośredniego od innych form marketingu. Przyjmuje się, że marketing bezpośredni służy informowaniu o możliwości bezpośredniego nabycia towarów lub usług oraz składania potencjalnym klientom propozycji zawarcia umów, tym samym nie obejmuje swym zakresem pojęciowym kontaktów z użytkownikami końcowymi, podejmowanych celem informowania o działalności przedsiębiorcy bez składania mu oferty handlowej i propozycji zawarcia umowy przez telefon.

Stanowiska tego nie poparł Prezes UOKIK Marek Niechciał, mówiąc, że „Przedsiębiorca musi mieć wcześniejszą zgodę na kontakt telefoniczny – nie tylko jeśli chce przedstawić swoją ofertę, ale także gdy chce ją tylko zapowiedzieć lub wybadać potrzeby klientów. Takiej zgody nie może uzyskać na początku rozmowy telefonicznej", co miało miejsce w postępowaniu wobec firmy ACS Medica ze Śremu[8].

Każdorazowo, zarówno w kontakcie telefonicznym, jak i mailowym, należy przestrzegać konieczności wysłania obowiązku informacyjnego. Odbiorca powinien wiedzieć, jakie przysługują mu prawa, że ma możliwość wycofania zarówno zgody, jak i zgłoszenia sprzeciwu.

Udowodnienie odebrania zgody w pierwszej rozmowie telefonicznej oraz przekazania obowiązku informacyjnego może nie być proste. Administrator powinien samodzielnie dobrać odpowiednie narzędzie na miarę swoich możliwości finansowych i technologicznych, np. nagrywanie rozmów, potwierdzenie w e-mailu.

Obowiązki związane z prawidłowym odebraniem zgody

Gdy zgoda na wysyłkę ofert handlowych zostanie odebrana w jeden ze sposobów przedstawionych wcześniej, należy pamiętać także o dalszych obowiązkach prawnych firmy.

Jedną z najważniejszych czynności, o której nie można zapomnieć, jest spełnienie obowiązku informacyjnego względem osoby, która udzieliła firmie zgody.

Klauzula informacyjna zgodna z art. 13 lub 14 RODO powinna zostać dostarczona odbiorcy w taki sposób, aby mógł zapoznać się on z jej treścią.

Zazwyczaj w przypadku odbierania zgody na wysyłkę ofert drogą elektroniczną pierwsza warstwa obowiązku informacyjnego prezentowana jest przy okazji checkboxa lub komunikatu.

W treści zgody odsyła się jednocześnie do tzw. drugiej warstwy obowiązku informacyjnego poprzez:

- link do polityki prywatności jako pełnego dokumentu zawierającego kwestie związane z ochroną danych na stronie firmy, na której pobiera się zgody,
- rozwijaną pełną treść klauzuli informacyjnej po kliknięciu w określony komunikat, np. czytaj więcej, rozwiń.

Brak spełnienia obowiązku informacyjnego skutkuje naruszeniem zasad ochrony prywatności i grozi karami wynikającymi z RODO, a także z polskich ustaw. Stanowi także ryzyko nałożenia wysokich kar pieniężnych, jak miało to już miejsce w kilku postępowaniach przed Prezesem Urzędu Ochrony Danych Osobowych[9].

Czy spółki handlowe i przedsiębiorcy wpisani do CEIDG są chronieni przez RODO?

Z motywu 14 RODO wynika, że rozporządzenie zapewnia ochronę osobom fizycznym niezależenie od ich obywatelstwa czy miejsca zamieszkania w związku z przetwarzaniem ich danych osobowych.

RODO nie dotyczy natomiast osób prawnych, czyli np. spółek prawa handlowego wpisanych do KRS i osób reprezentujących te spółki, np. członków zarządu.

Jeśli chodzi o przedsiębiorców wpisanych do CEIDG, czyli tzw. jednoosobowych działalności gospodarczych, których jest w Polsce przeważająca liczba, sytuacja nie była już taka klarowna. Komisja Europejska potwierdziła jednak, że dane jednoosobowych przedsiębiorców (w tym ich adresy e-mail) są chronione przez RODO. Dane osób prawnych i ich przedstawicieli nie[10].

Stało się więc pewne, że wobec jednoosobowych przedsiębiorców należy

zrealizować obowiązek informacyjny, jak również odebrać zgody na wysyłkę ofert handlowych w sposób odpowiadający wymogom RODO.

Z kolei w stosunku do osób prawnych, np. spółek prawa handlowego, problem pojawił się całkiem niedawno w stanowisku Prezesa UODO[11]. Oparł się on m.in. na odpowiedzi Komisji Europejskiej na inne pytanie w sprawie adresów e-mail osób prawnych i ich pracowników, a także na wyroku TSUE[12]. Uznał, że „dane członków zarządu reprezentujących osobę prawną, dane pełnomocników osób prawnych, a także dane pracowników, którzy są osobami kontaktowymi osoby prawnej, będących możliwymi do zidentyfikowania osobami fizycznymi, będą danymi osobowymi podlegającymi ochronie RODO. Wobec tego administrator jest zobligowany do wypełnienia w stosunku do takich osób obowiązku informacyjnego określonego w art. 13 lub 14 RODO, o ile nie zachodzi jedna z przesłanek zwalniających go z tego obowiązku".

Pokazuje to, że sprawa nie jest prosta, pomimo że osoby prawne nie są chronione przez RODO, ale żeby uprościć swoje obowiązki związane z pozyskiwaniem zgód i wysyłaniem klauzuli informacyjnej najlepiej robić to w stosunku do przedsiębiorców z CEIDG i jednocześnie spółek prawa handlowego czy osób prawnych, tzn. ich pracowników czy przedstawicieli.

Czy upsell jest dopuszczalny i na jakiej podstawie?

Wielu przedsiębiorców zastanawia się, czy dopuszczalny jest tzw. upsell, czyli przesyłanie ofert handlowych dotychczasowym klientom.

Jeśli chodzi o RODO, tak jak zostało wspomniane, byłoby to możliwe na podstawie prawnej uzasadnionego interesu administratora (art. 6 ust. 1 lit. f RODO) i wykonaniu tzw. testu równowagi (najlepiej w formie pisemnej lub elektronicznej, aby zrealizować zasadę rozliczalności) w celu marketingu bezpośredniego. Może to być na przykład wysłanie do swoich klientów drogą pocztową życzeń i kodu rabatowego[13].

Biorąc jednak pod uwagę przepisy UŚUDE, o którym była już mowa, na wysyłkę ofert marketingowych drogą elektroniczną (e-mailem) potrzebna jest wyraźna zgoda.

Najlepiej odebrać ją w procesie zakupowym, w którym klient będzie miał możliwość zaznaczenia zgody na wysyłkę ofert handlowych albo co jakiś czas dać klientom możliwość pobrania bezpłatnie wartościowych materiałów w zamian za zgodę na taką komunikację. Wymóg dobrowolności zostanie tutaj zachowany, gdyż pojawi się świadczenie wzajemne (w postaci tzw. lead magnetu), mające obustronnie charakter niepieniężny[14].

Należy jednak pamiętać, aby każdorazowo dać możliwość łatwego wycofania zgody i przesłać klauzulę informacyjną.

Planowane e-Privacy i PKE

Na koniec należy także wspomnieć o nadchodzących zmianach w zakresie pozyskiwania zgód marketingowych. Unia Europejska idzie w kierunku zmniejszenia liczby zgód na wysyłkę ofert, czego jednak nie chce zrobić polski ustawodawca. W projekcie nowego Prawa Komunikacji Elektronicznej wskazuje się na konieczność uprzedniego uzyskiwania zgód[15]. Rozporządzenie e-Privacy, które ciągle jest w fazie projektu, jest bardziej liberalne w tym zakresie, a jeśli ujrzy światło dzienne, to będzie stosowane wprost w Polsce. Tego oczekują polscy przedsiębiorcy w celu ułatwienia marketingu swoich produktów i usług.

Podsumowanie

Wysyłka ofert handlowych drogą mailową jest bardzo popularna i potrafi być niezwykle skuteczna. Jeśli do budowania bazy mailingowej podejdzie się bazując na przepisach prawnych i realizując podstawowe obowiązki, można czerpać z tego bardzo duże korzyści. I to nie będą korzyści tylko dla przedsiębiorcy, ale także dla samych klientów. Warto zaplanować procesy pozyskiwania potencjalnych klientów i budowania społeczności zgodnie z prawem i RODO.

Ilona Przetacznik
radca prawny, project manager oraz lean lider, prowadzi blog legalnybiznesonline.pl

1 Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców, https://uodo.gov.pl/pl/138/545.
2 Kodeks postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej – projekt do konsultacji publicznych, IAB Polska źródło: https://iab.org.pl/wp-content/uploads/2018/08/Kodeks-postępowania-RODO_IAB-Polska_projekt-do-konsultacji.pdf.
3 RODO. Poradnik dla sektora FinTech. Ministerstwo Cyfryzacji.
4 Motyw 42 i 43 RODO wskazuje na cechy prawidłowo uzyskanej zgody oraz elementy jej dobrowolności.
5 RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, pod redakcją Dominika Lubasza, stan prawny: 1 października 2017 r., teza 355–356.
6 RODO. Poradnik dla sektora FinTech. Ministerstwo Cyfryzacji.
7 Kodeks postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej – projekt do konsultacji publicznych, IAB Polska źródło: https://iab.org.pl/wp-content/uploads/2018/08/Kodeks-postępowania-RODO_IAB-Polska_projekt-do-konsultacji.pdf.
8 https://www.uokik.gov.pl/aktualnosci.php?news_id=14949.
9 Decyzją z 15 marca 2019 r. o sygnaturze akt ZSPR.421.3.2018 Prezes Urzędu Ochrony Danych Osobowych nałożył karę pieniężną w wysokości 943 470,00 zł m.in. z tytułu niespełnienia obowiązku informacyjnego wobec niektórych klientów firmy (głównie prowadzących jednoosobową działalność gospodarczą oraz tych, którzy taką działalność w przeszłości zawiesili). Decyzją z dnia 16 października 2019 r., o sygnaturze akt ZSPR.421.7.2019 Prezes Urzędu Ochrony Danych Osobowych nałożył administracyjną karę pieniężną w wysokości 201 559,50 zł na spółkę ClickQuickNow z powodu utrudniania wycofywania zgody na działania marketingowe. Źródło: https://uodo.gov.pl/decyzje/ZSPR.421.7.2019. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 grudnia 2019 r. II SA/Wa 1030/19, LEX nr 2759399 w sprawie Bisnode.
10 Odpowiedź Komisji Europejskiej na pytanie „Czy przepisy o ochronie danych mają zastosowanie do danych dotyczących przedsiębiorstwa?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_pl.
11 Stanowisko Prezesa UODO i odpowiedź na pytanie „Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?", https://uodo.gov.pl/pl/225/1577.
12 Odpowiedź Komisji Europejskiej na pytanie nr E-007174/2017, https://www.europarl.europa.eu/doceo/document/E-8-2017-007174-ASW_EN.html?redirect, oraz Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 9 marca 2017 r. w sprawie C-398/15, https://curia.europa.eu/juris/documents.jsf?num=C-398/15.
13 Ochrona Danych Osobowych. Meritum pod redakcją naukową Dominika Lubasza, Wolters Kluwer, Warszawa 2020, teza 261–263.
14 E-mail marketing kontra RODO, Barbara Chabior, Raport E-mail marketing, Interaktywnie.com, lipiec 2018.
15 https://www.prawo.pl/biznes/zgoda-na-przeslanie-firmie-oferty-ue-rezygnuje-z-tego-wymogu,506418, https://www.prawo.pl/biznes/zgoda-marketingowa-na-kazdy-kanal-komunikacji-projekt-pke,506641.html.

Świadczenie pracy zdalnej przez cudzoziemca

Najważniejsze zagadnienia w czasie pandemii

dr Małgorzata Mędrala

Świadczenie pracy zdalnej staje się coraz bardziej popularne w stosunkach pracy z elementem transgranicznym, a pandemia COVID-19 jeszcze bardziej nasiliła to zjawisko. Coraz więcej firm zagranicznych zatrudnia polskich pracowników w formie telepracy lub kieruje ich na pracę zdalną. Wielu polskich pracodawców korzysta także z pracy cudzoziemców na odległość.

Praca zdalna w szczególności sprawdza się w przypadku programistów, pracowników firm informatycznych, niektórych pracowników biurowych, kadry menedżerskiej, grafików czy dziennikarzy. Należy przy tym odróżnić dwie formy zdalnego świadczenia pracy uregulowane w obecnych przepisach prawa polskiego:

- telepracę regulowaną przepisami kodeksu pracy (art. 67^5 – 67^{17} k.p.), cechującą się stałością i regularnością świadczenia pracy w tym trybie;
- pracę zdalną uregulowaną w ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020 r. poz. 1842), zwaną dalej ustawą covidową, będącą z założenia rozwiązaniem przejściowym, stosowanym w trybie polecenia pracodawcy i realizującym cele zdrowotne (przeciwdziałanie COVID-19) oraz ochrony miejsc pracy.

W przypadku pracy zdalnej i telepracy możliwe jest jej świadczenie przez cudzoziemca zarówno na terenie Polski (w innym miejscu niż do tej pory ustalone), jak również poza jej granicami, w tym z miejsca zamieszkania pracownika. Powyższe rodzi szereg pytań natury praktycznej, z którymi na co dzień muszą zmierzyć się pracodawcy. W artykule poruszone zostaną zagadnienia z zakresu ważności dotychczasowych pozwoleń na pracę, prawa właściwego, oskładkowania i opodatkowania wynagrodzenia pracownika cudzoziemca, zatrudnienia pracowników będących obywatelami EOG/Szwajcaria i obywateli państw trzecich – z perspektywy różnic w kontekście ustawy covidowej, przedłużenia legalności pobytu pracowników z państw trzecich, jak również zezwoleń na pracę sezonową.

Praca zdalna a zezwolenie na pracę

W pierwszej kolejności pojawia się **pytanie o legalność pracy zdalnej cudzoziemca z perspektywy posiadanego zezwolenia na pracę**. Zasadą jest, iż wykonywanie na terenie Polski pracy przez cudzoziemca spoza krajów Unii Europejskiej wymaga zezwolenia na pracę. Miejsce świadczenia pracy przez cudzoziemca nie jest wymienione w samym zezwoleniu na pracę, ale należy je wskazać we wniosku o jego wydanie (art. 88 ust. 1aa pkt 4 lit. c ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, Dz.U. z 2020 r. poz. 1409). Miejsce świadczenia pracy przez cudzoziemca wskazuje się także w oświadczeniu o powierzeniu wykonywania pracy cudzoziemcowi wpisanym do ewidencji oświadczeń (zob. art. 88z ust. 1 pkt 3 lit. c ustawy o promocji zatrudnienia).

W ustawie covidowej przesądzono jednak możliwość pracy zdalnej cudzoziemców, niezależnie od wskazania miejsca wykonywania pracy we wniosku o wydanie zezwolenia, lub w samym oświadczeniu o powierzeniu wykonywania pracy cudzoziemcowi wpisanym do ewidencji oświadczeń. Zgodnie z art. $15z^5$ ustawy covidowej, jeżeli na skutek skorzystania przez podmiot powierzający wykonywanie pracy cudzoziemcowi, z uprawnień określonych m.in. w art. 3 ustawy covidowej uległy zmianie warunki wykonywania pracy przez cudzoziemca określone w:

1) zezwoleniu na pobyt czasowy i pracę,
2) zezwoleniu na pobyt czasowy w celu wykonywania pracy w zawodzie wymagającym wysokich kwalifikacji,
3) zezwoleniu na pracę,
4) zezwoleniu na pracę sezonową,
5) oświadczeniu o powierzeniu wykonywania pracy cudzoziemcowi wpisanym do ewidencji oświadczeń na podstawie art. 88z ust. 2 ustawy o promocji zatrudnienia

– cudzoziemiec może wykonywać pracę na tych zmienionych warunkach bez konieczności zmiany zezwolenia, uzyskania nowego zezwolenia lub wpisania nowego oświadczenia o powierzeniu wykonywania pracy cudzoziemcowi do ewidencji oświadczeń.

W przypadku pracy na podstawie oświadczenia o powierzeniu wykonywania pracy zaleca się, aby ze względów dowodowych polecenie wykonywania przez cudzoziemca pracy zdalnej zostało udokumentowane, np. w postaci skierowanego do pracownika e-maila zawierającego takie polecenie i okres świadczenia pracy zdalnej.

W przypadku stałej, regularnej pracy zdalnej cudzoziemca za granicą nie jest wymagane polskie zezwolenie na pracę, gdyż wymóg jego uzyskania istnieje jedynie w przypadku pracy na terenie Polski. Konieczne jest jednak zawsze zbadanie przepisów lokalnych w tym zakresie. Zwrócić należy przy tym uwagę, iż w przypadku niektórych państw, jak np. Barbados, przewidziano specjalne wizy do świadczenia pracy zdalnej z ich terytorium.

Prawo właściwe

O ile w przypadku pracy zdalnej w dotychczasowym kraju, zwłaszcza w Polsce, nie ulega zmianie dotychczasowe

ustawodawstwo krajowe, któremu podlegał pracownik, o tyle w przypadku telepracy lub pracy zdalnej powiązanej ze stałą lub czasową zmianą miejsca pracy pojawić się może pytanie o ustawodawstwo danego kraju, któremu stosunek pracy podlega. W przypadku pracy zdalnej cudzoziemców zastosowanie znajdzie rozporządzenie unijne „Rzym I" (rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 w sprawie prawa właściwego dla zobowiązań umownych, Dz.U.UE.L.2008.177.6):

1) Zgodnie z art. 8 tegoż rozporządzenia, indywidualna umowa o pracę podlega prawu wybranemu przez strony zgodnie z art. 3. Taki wybór prawa nie może jednak prowadzić do pozbawienia pracownika ochrony przyznanej mu na podstawie przepisów, których nie można wyłączyć w drodze umowy, na mocy prawa, jakie, w przypadku braku wyboru, byłoby właściwe zgodnie z przepisami rozporządzenia. W przypadku pracy zdalnej cudzoziemca oznacza to konieczność zapewnienia minimalnego standardu ochrony i warunków zatrudnienia, jakie przewiduje kraj, w którym cudzoziemiec świadczy pracę.
2) Z kolei w zakresie, w jakim strony nie dokonały wyboru prawa właściwego dla indywidualnej umowy o pracę, umowa podlega prawu państwa, w którym lub – gdy takiego brak – z którego pracownik zazwyczaj świadczy pracę w wykonaniu umowy. Za zmianę państwa, w którym zazwyczaj świadczona jest praca, nie uważa się tymczasowego zatrudnienia w innym państwie.
3) Jeżeli nie można ustalić prawa właściwego zgodnie z powyższą regułą, umowa podlega prawu państwa, w którym znajduje się przedsiębiorstwo, za pośrednictwem którego zatrudniono pracownika. Jeżeli ze wszystkich okoliczności wynika, że umowa wykazuje ściślejszy związek z innym państwem, stosuje się prawo tego innego państwa.

Kwestie podatkowe i składkowe pracy cudzoziemca regulowane są przede wszystkim przez przepisy lokalne miejsca wykonywania pracy, jak również umowy międzynarodowe o unikaniu podwójnego opodatkowania oraz oskładkowania.

Składki ZUS

W kontekście oskładkowania pojawia się pytanie, czy należy opłacać składki ZUS, jeżeli pracownik cudzoziemiec wykonuje pracę zdalną poza Polską. Podkreślić przy tym należy, iż problemu tego nie ma, jeśli praca zdalna jest nadal wykonywana przez cudzoziemca na terytorium Polski. Istnieje duże prawdopodobieństwo powstania obowiązku składkowego w państwie, gdzie praca (zdalna) jest faktycznie wykonywana.

W kwestiach oskładkowania przychodów pracownika-cudzoziemca pracującego zdalnie należy w pierwszej kolejności odwołać się do przepisów polskiej ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, Dz.U. z 2021 r., poz. 423, dalej: ustawa systemowa. Zgodnie z jej art. 6 ust. 1 pkt. 1 obowiązkowo ubezpieczeniom emerytalnym i rentowym podlegają, z zastrzeżeniem art. 8 i 9, **osoby fizyczne, które na obszarze Rzeczypospolitej Polskiej są pracownikami**. Zgodnie z art. 5 ust. 2 ustawy systemowej nie podlegają ubezpieczeniom społecznym określonym w ustawie obywatele państw obcych, których pobyt na obszarze Rzeczypospolitej Polskiej nie ma charakteru stałego i którzy są zatrudnieni w obcych przedstawicielstwach dyplomatycznych, urzędach konsularnych, misjach, misjach specjalnych lub instytucjach międzynarodowych, chyba że umowy międzynarodowe stanowią inaczej.

Tym samym ustawą nie są objęci pracownicy–cudzoziemcy, którzy nie wykonują pracy na terenie Polski, jak również nie mają miejsca zamieszkania na terenie Polski. Ważne w tym przypadku jest jednak jasne ustalenie, że miejscem pracy pracownika (pracy zdalnej) nie jest Polska. Nie chodzi przy tym o przypadki podróży służbowych za granicę z Polski. Jak wskazuje ZUS, „**polskim przepisom o ubezpieczeniach społecznych nie podlegają również cudzoziemcy zatrudnieni wprawdzie przez polskie podmioty, ale miejsce wykonywania ich pracy określono poza granicami Polski. Jeśli bowiem miejsce pracy zostało określone za granicą i tam praca jest wykonywana, to zatrudniony cudzoziemiec nie jest pracownikiem na obszarze Polski**". Brakuje bowiem wtedy łącznika w zakresie oskładkowania, jakim jest miejsce pracy na terenie RP.

Wykonywanie pracy zdalnej nie stanowi przy tym oddelegowania, w którego to przypadku jest możliwość uzyskania zaświadczenia A1 o podleganiu ubezpieczeniom społecznym dotychczasowego państwa. Art. 12 Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 883/2004 w sprawie koordynacji systemów zabezpieczenia społecznego, Dz.U. L 166, 30.4.2004, p. 1 (dalej: rozporządzenie 883/2004) przewiduje bowiem możliwość uzyskania zaświadczenia A1 o podleganiu ustawodawstwu ubezpieczeniowemu dotychczasowego państwa członkowskiego w przypadku tymczasowego oddelegowania pracownika w celu świadczenia usług. Przy pracy zdalnej nie mamy jednak do czynienia z oddelegowaniem w celu świadczenia usług w innym kraju. Podobnie nie znajdzie zastosowania art. 13 tegoż rozporządzenia, który odnosi się do pracy wykonywanej na terenie kilku państw członkowskich. Praca będzie bowiem wykonywana na ogół w jednym państwie za granicą. Jedyną możliwością pozostania przy dotychczasowym (polskim) systemie ubezpieczeniowym jest zatem **wystąpienie w trybie art. 16 rozporządzenia do oddziału ZUS w Kielcach, o zawarcie porozumienia wyjątkowego pomiędzy dwoma państwami członkowskimi. W przeciwnym wypadku pracownik będzie podlegał ubezpieczeniom społecznym państwa, gdzie praca (zdalna) jest faktycznie wykonywana przez niego**.

Z kolei w przypadku państw trzecich, istotne jest **zbadanie odpowiedniej umowy dotyczącej zabezpieczenia społecznego, z danym państwem trzecim**, w którym pracownik wykonuje zdalnie pracę. Jeżeli takiej umowy nie ma lub nie reguluje ona kwestii zbiegu podstaw tytułów ubezpieczeniowych, niewykluczone pozostaje podwójne oskładkowanie.

Podatek od wynagrodzenia

W przypadku zdalnego świadczenia pracy przez cudzoziemca z zagranicy może dojść do utraty polskiej rezydencji podatkowej. Dotyczy to zarówno

obywateli krajów Unii Europejskiej, jak i państw trzecich. Należy zwrócić przy tym uwagę, iż zgodnie z art. 3 ust. 1–1a ustawy o podatku dochodowym od osób fizycznych z dnia 26 lipca 1991 r., Dz.U. z 2020 r. poz. 1426, dalej: u.p.d.o.f., osoby fizyczne, **jeżeli mają miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej**, podlegają obowiązkowi podatkowemu od całości swoich dochodów (przychodów), **bez względu na miejsce położenia źródeł przychodów (nieograniczony obowiązek podatkowy)**.

Za osobę mającą miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej uważa się przy tym osobę fizyczną, która:

- **posiada na terytorium Rzeczypospolitej Polskiej centrum interesów osobistych lub gospodarczych (ośrodek interesów życiowych)**

lub

- **przebywa na terytorium Rzeczypospolitej Polskiej dłużej niż 183 dni w roku podatkowym**.

Z kolei zgodnie z art. 3 ust. 2a u.p.d.o.f. **osoby fizyczne, jeżeli nie mają na terytorium Rzeczypospolitej Polskiej miejsca zamieszkania, podlegają obowiązkowi podatkowemu tylko od dochodów (przychodów) osiąganych na terytorium Rzeczypospolitej Polskiej (ograniczony obowiązek podatkowy)**. Zgodnie z art. 3 ust. 2b pkt 1 u.p.d.o.f. za dochody (przychody) osiągane na terytorium Rzeczypospolitej Polskiej przez podatników, uważa się w szczególności dochody (przychody) **z pracy wykonywanej na terytorium Rzeczypospolitej Polskiej** na podstawie stosunku służbowego, stosunku pracy, pracy nakładczej oraz spółdzielczego stosunku pracy, bez względu na miejsce wypłaty wynagrodzenia.

W każdym przypadku zdalnego pracownika cudzoziemca konieczne będzie ustalenie, gdzie faktycznie osiąga dochody (przychody) ze stosunku pracy i czy praca jest wykonywana na terytorium Polski. Nie jest także wykluczona kolizja przepisów w zakresie lokalnej rezydencji podatkowej oraz przepisów o ograniczonym obowiązku podatkowym w Polsce. Dlatego też w tym kontekście bardzo ważna pozostaje **weryfikacja przepisów lokalnych miejsca wykonywania pracy oraz stosownej umowy o unikaniu podwójnego opodatkowania z danym państwem.** Ogólną zasadą w międzynarodowych umowach o unikaniu podwójnego opodatkowania jest to, iż dochody z pracy podlegają opodatkowaniu w miejscu zamieszkania podatnika, chyba że praca jest wykonywana w innym państwie. W przypadku braku umowy o podwójnym opodatkowaniu możliwe jest także podwójne opodatkowanie.

W przypadku pracowników cudzoziemców na ogół centrum interesów życiowych będzie leżeć poza Polską, ponadto z reguły będą oni przebywać poza terytorium RP ponad 183 dni w roku podatkowym. W dobie COVID-19 nie są jednak wykluczone sytuacje odwrotne. Dotyczyć to może zwłaszcza pracowników cudzoziemców, którzy wcześniej zmienili swój ośrodek życiowy na Polskę, a następnie ze względu na pandemię zdecydowali się na powrót do państwa rodzinnego. W takiej sytuacji może dojść do czasowej lub stałej zamiany rezydencji polskiej na zagraniczną. Nie można przy tym zapominać, że w przypadku telepracy mamy do czynienia z regularnym, stałym wykonywaniem pracy na odległość z ustalonego miejsca. W przypadku pracy zdalnej polecenie pracy w tym trybie jest z założenia czasowe i może być zmienne.

Zatrudnianie pracowników będących obywatelami EOG/Szwajcarii i obywateli państw trzecich – różnice w kontekście ustawy covidowej

W przypadku zatrudnienia obywateli państw Unii Europejskiej zasady zatrudnienia w dobie COVID-19 nie uległy zasadniczo zmianie. W ich przypadku nie jest bowiem wymagane zezwolenie na pracę.

Ustawa covidowa przedłużyła jednocześnie z mocy prawa okresy ważności dokumentów wydawanych na czas określony obywatelom państw członkowskich UE, Europejskiego Porozumienia o Wolnym Handlu (EFTA), Konfederacji Szwajcarskiej i przebywających z nimi członków rodzin, tj.:

- dokumentów potwierdzających prawo stałego pobytu,
- kart pobytu członka rodziny obywatela UE,
- kart stałego pobytu członka rodziny obywatela UE.

Problem pojawia się natomiast w zakresie legalności zatrudniania cudzoziemców państw trzecich, dla których podstawą zatrudnienia jest **zezwolenie na pracę lub oświadczenie o powierzeniu wykonywania pracy, wraz z zezwoleniem na pobyt**. Ze względu na fakt, iż decyzje w tym zakresie mogą się kończyć w okresie pandemii i mogą istnieć problemy z ich przedłużeniem, ustawa covidowa *ex lege* przedłuża ich ważność. Przedłużenie dotyczy ważności wszystkich zezwoleń na pracę.

W myśl art. 15zzq ustawy covidowej, jeżeli ostatni dzień ważności zezwolenia na pracę, o którym mowa w art. 88 ust. 1 pkt 1–5 lub ust. 2 ustawy o promocji zatrudnienia, przypada w okresie stanu zagrożenia epidemicznego lub stanu epidemii, ogłoszonego w związku z zakażeniami wirusem SARS-CoV-2, **okres ważności tego zezwolenia na pracę ulega przedłużeniu z mocy prawa do upływu 30. dnia następującego po dniu odwołania tego ze stanów, który obowiązywał jako ostatni**. Dotyczy to także odpowiednio decyzji o przedłużeniu zezwolenia na pracę lub przedłużeniu zezwolenia na pracę sezonową. Ponadto, w przypadku przedłużenia okresu ważności zezwolenia na pracę na tej podstawie, wniosek o przedłużenie zezwolenia na pracę, składa się nie wcześniej niż w terminie 90 dni przed upływem okresu ważności zezwolenia na pracę określonego w tym zezwoleniu i nie później niż w ostatnim dniu okresu ważności zezwolenia przedłużonego na tej podstawie.

Podobnie jeżeli w oświadczeniu o powierzeniu wykonywania pracy cudzoziemcowi, wpisanym do ewidencji oświadczeń na podstawie art. 88z ust. 2 ustawy o promocji zatrudnienia, wskazano okres pracy, którego koniec przypada w okresie stanu zagrożenia epidemicznego lub stanu epidemii, ogłoszonego w związku z zakażeniami wirusem SARS-CoV-2, cudzoziemiec może wykonywać pracę określoną oświadczeniem na rzecz podmiotu, który złożył oświadczenie, w okresie lub okresach

nieobjętych oświadczeniem, do upływu 30. dnia następującego po dniu odwołania tego ze stanów, który obowiązywał jako ostatni, bez zezwolenia na pracę.

W ustawie przesądzono także **możliwość pracy zdalnej cudzoziemców, pomimo wskazania miejsca wykonywania pracy we wniosku o wydanie zezwolenia lub w oświadczeniu o powierzeniu wykonywania pracy cudzoziemcowi wpisanym do ewidencji oświadczeń**, jak również **pomimo zmiany wymiaru czasu pracy czy obniżenia wynagrodzenia na skutek zawarcia antykryzysowych porozumień zbiorowych przewidzianych ustawą covidową**. W takim przypadku nie jest konieczna zmiana zezwolenia na pracę lub wpisanie nowego oświadczenia o powierzeniu wykonywania pracy cudzoziemcowi do ewidencji oświadczeń (zob. art. 15z[5] ust. 1 ustawy covidowej).

Przedłużenie legalności pobytu pracowników z państw trzecich

Przepisy ustawy covidowej przewidują specjalne regulacje dla cudzoziemców (obywateli państw trzecich), których legalny pobyt na terytorium Rzeczypospolitej Polskiej uległby zakończeniu w okresie stanu zagrożenia epidemicznego lub stanu epidemii. Nie dotyczy to obywateli państw Unii Europejskiej, albowiem w ich przypadku pobyt nie wymaga specjalnego zezwolenia.

Po pierwsze, **przedłużone zostają terminy na składanie wniosków związanych z zezwoleniami pobytowymi oraz w sprawach przedłużenia wiz krajowych i pobytu w ruchu bezwizowym**, wypadające w okresie stanu zagrożenia epidemicznego lub stanu epidemii. Zgodnie z art. 15z ustawy covidowej powoduje to automatyczne przedłużenie terminów na składanie wniosków o:

- udzielenie zezwolenia na pobyt czasowy, tj. terminu określonego w art. 105 ust. 1 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz.U. z 2020 r. poz. 35),
- udzielenie zezwolenia na pobyt stały, tj. terminu określonego w art. 202 ust. 1 ustawy o cudzoziemcach,
- udzielenie zezwolenia na pobyt rezydenta długoterminowego UE, tj. terminu określonego w art. 202 ust. 1, a stosowanego na mocy odesłania zawartego w art. 223 ustawy o cudzoziemcach,
- przedłużenie wizy, tj. terminu określonego w art. 85 ust. 1 ustawy o cudzoziemcach,
- przedłużenie pobytu w ramach ruchu bezwizowego, tj. terminu określonego w art. 300 ust. 2 ustawy o cudzoziemcach).

Termin ten ulega przedłużeniu do upływu 30. dnia następującego po dniu odwołania tego ze stanów, który obowiązywał jako ostatni. Umożliwia to cudzoziemcom dopełnienie wymogu osobistego złożenia wniosku w ww. sprawach w terminach, jakie wyznacza ich dotychczasowy legalny pobyt, względnie osobiste stawiennictwo na wezwanie organu, eliminując ryzyko popadnięcia w nielegalny pobyt w aktualnej sytuacji czasowego zawieszenia bezpośredniej obsługi klienta przez urzędy wojewódzkie.

Ponadto, zgodnie z art. 15z[1] ust. 1 ustawy covidowej w przypadku cudzoziemca, który w dniu, od którego po raz pierwszy ogłoszono stan zagrożenia epidemicznego w związku z zakażeniami wirusem SARS-CoV-2, przebywał na terytorium Rzeczypospolitej Polskiej:

1) na podstawie wizy Schengen,
2) na podstawie wizy wydanej przez inne państwo obszaru Schengen,
3) na podstawie dokumentu pobytowego wydanego przez inne państwo obszaru Schengen,
4) w ramach ruchu bezwizowego,
5) na podstawie wizy długoterminowej wydanej przez inne państwo członkowskie Unii Europejskiej niebędące państwem obszaru Schengen, jeżeli zgodnie z przepisami prawa Unii Europejskiej uprawnia ona do pobytu na terytorium Rzeczypospolitej Polskiej,
6) na podstawie dokumentu pobytowego wydanego przez inne państwo członkowskie Unii Europejskiej niebędące państwem obszaru Schengen, jeżeli zgodnie z przepisami prawa Unii Europejskiej uprawnia ona do pobytu na terytorium Rzeczypospolitej Polskiej

– jego pobyt na tym terytorium uważa się za legalny od dnia następującego po ostatnim dniu legalnego pobytu wynikającego z tych wiz, dokumentów lub ruchu bezwizowego, do upływu 30. dnia następującego po dniu odwołania stanu zagrożenia epidemicznego albo stanu epidemii, w zależności od tego, który obowiązywał jako ostatni.

Cudzoziemcy jw. są uprawnieni do wykonywania pracy na terytorium Rzeczypospolitej Polskiej w ww. okresie pobytu uznawanego za legalny, jeżeli posiadają:

- ważne zezwolenie na pracę lub ważne zezwolenie na pracę sezonową;
- oświadczenie o powierzeniu wykonywania pracy wpisane do ewidencji oświadczeń.

Zaznaczyć przy tym należy, że **nie dotyczy to cudzoziemców, którzy na podstawie wskazanych dokumentów wjechali na teren RP po dniu 14 marca 2020 r.**

Cudzoziemiec objęty jest tym rozwiązaniem automatycznie, bez konieczności składania dodatkowych dokumentów.

Przedłużeniu do 30 dni po odwołaniu stanu epidemii lub stanu zagrożenia epidemicznego ulega także ważność kart pobytu oraz ważność tymczasowych zaświadczeń tożsamości cudzoziemców, jeżeli okres ważności upłynął w czasie stanu zagrożenia epidemicznego lub stanu epidemii (art. 15z[2] ustawy covidowej).

Analogiczne rozwiązanie co do przedłużenia ważności do upływu 30. dnia następującego po dniu odwołania tego ze stanów, który obowiązywał jako ostatni, ustawodawca przewidział dla cudzoziemców, których okres legalnego pobytu wynikającego z **zezwoleń na pobyt czasowy lub wiz krajowych** (tj. wiz długoterminowych wydanych przez konsuli RP, wizy typu „D") wypada w okresie stanu zagrożenia epidemicznego lub stanu epidemii (15zd ustawy covidowej). W takim przypadku w dokumencie podróży cudzoziemca nie umieszcza się nowej naklejki wizowej.

Ponadto, na mocy ustawy covidowej, przesunięte zostają terminy opuszczenia terytorium Polski wynikające z art. 299 ust. 6 ustawy o cudzoziemcach oraz dobrowolnego powrotu określonego w decyzji o zobowiązaniu cudzoziemca do powrotu, w przypadku którego data końcowa wypadałaby w okresie stanu zagrożenia epidemicznego lub stanu epidemii. Przedłużenie następuje również do upływu 30. dni od zakończenia stanu epidemii lub stanu zagrożenia epidemicznego, w zależności od tego, który z nich obowiązywał ostatni.

Zezwolenia na pracę sezonową

Dodatkowe ułatwienia zostały także wprowadzone w przypadku zezwoleń na pracę sezonową.

Przepis art. 15z[7] ustawy covidowej stanowi, iż zezwolenie na pracę, nie jest wymagane w czasie stanu zagrożenia epidemicznego albo stanu epidemii ogłoszonych w związku z COVID-19 oraz do 30. dnia następującego po odwołaniu tego ze stanów, który obowiązywał jako ostatni, jeżeli cudzoziemiec wykonuje pracę w zakresie podklas działalności według klasyfikacji PKD, w których wydaje się zezwolenia na pracę sezonową oraz posiadał:

1) zezwolenie na pracę, ważne po dniu 13 marca 2020 r. (w tym także decyzję o przedłużeniu zezwolenia na pracę lub przedłużeniu zezwolenia na pracę sezonową)

lub

2) oświadczenie o powierzeniu wykonywania pracy cudzoziemcowi wpisane do ewidencji oświadczeń, w którym przynajmniej jeden dzień okresu pracy określonego w tym oświadczeniu przypada po dniu 13 marca 2020 r.

Ustawa przewiduje więc automatyczne przedłużenie możliwości pracy na podstawie dokumentów, których koniec ważności przypada w okresie stanu zagrożenia epidemicznego lub stanu epidemii.

Podsumowanie

Jak wynika z powyższej analizy, zdalne świadczenie pracy przez cudzoziemca rodzi szereg problemów natury praktycznej. O ile ustawodawca rozwiązał w sposób dość jednoznaczny kwestie legalności ich pobytu oraz pracy w kontekście kończących się zezwoleń na pracę czy zezwoleń na pobyt na terenie RP w okresie pandemicznym, o tyle znacznie więcej trudności w praktyce może sprawiać ich zdalne świadczenie pracy z zagranicy na gruncie przepisów zabezpieczenia społecznego oraz podatkowych. Przede wszystkim wymaga to drobiazgowej analizy nie tylko przepisów krajowych, ale także ustawodawstwa lokalnego i umów o unikaniu podwójnego opodatkowania, jak również oskładkowania.

dr Małgorzata Mędrala
radca prawny, odpowiedzialna za dział prawa pracy w Kancelarii BDO Legal Łatała i Wspólnicy

1 Szerzej: M. Mędrala, Praca zdalna a wykluczenie społeczne (w:) Praca zdalna w polskim systemie prawa pracy, red. M. Mędrala, Warszawa 2021 (w druku) oraz cytowana tam pozycja D. Makowski, Kilka uwag o pracy zdalnej, PiZS 2020, nr 10, s. 13 i n.
2 U. Mirowska-Łoskot, Praca w domu też dla cudzoziemca, DGP z 11 lutego 2021 r.
3 Zob. art. 88 ustawy o promocji zatrudnienia i instytucjach rynku pracy z 20 kwietnia 2004 r. (t.j. Dz.U. z 2020 r. poz. 1409; por. A. Kałwińska, Praca zdalna z zagranicy. O czym muszą pamiętać pracodawcy? DGP z 25 lutego 2021 r.
4 Zob. Ubezpieczenia społeczne i ubezpieczenie zdrowotne Polaków zatrudnionych za granicą oraz cudzoziemców pracujących w Polsce. Poradnik, Zakład Ubezpieczeń Społecznych 2016 r.
5 https://udsc.gov.pl/pobyt-obywateli-ue-eog-szwajcarii-a-epidemia-koronawirusa/ (dostęp: 8 kwietnia 2021 r.).
6 Zob. art. art. 15g ust. 8 ustawy covidowej, który przewiduje możliwość obniżenia wymiaru czasu pracy, art. 15x ust. 1 ustawy covidowej, który przewiduje szczególne rozwiązania w zakresie uelastycznienia czasu pracy w dobie COVID, m.in. zmiany systemu i rozkładu czasu pracy lub art. 15zf ust. 1 ustawy covidowej, który przewiduje m.in. możliwość zawarcia porozumienia o stosowaniu mniej korzystnych warunków zatrudnienia.
7 Ruch bezwizowy obowiązuje m.in. dla obywateli: Albanii (tylko dla posiadaczy paszportów biometrycznych), Argentyny, Australii, Austrii, Brazylii, Izraela, Japonii, Kanady, Korei Południowej, Litwy, Łotwy, Meksyku, USA, Ukrainy, Mołdawii, Zjednoczonych Emiratów Arabskich – zob. Lista państw, których obywatele mogą podróżować do Polski bez wiz https://www.gov.pl/web/gruzja/lista-panstw-ktorych-obywatele-moga-podrozowac-do-polski-bez-wiz (dostęp: 8 kwietnia 2021 r.).
8 https://www.gov.pl/web/gov/przedluzenie-terminow-zwiazanych-ze-skladaniem-wnioskow-o-pozwolenia-na-pobyt-w-polsce (dostęp: 8. kwietnia 2021 r.).
9 https://www.gov.pl/web/gov/przedluzenie-terminow-zwiazanych-ze-skladaniem-wnioskow-o-pozwolenia-na-pobyt-w-polsce (dostęp: 18 marca 2021 r.).
10 Na podstawie rozporządzenia Ministra Zdrowia z dnia 13 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu zagrożenia epidemicznego, stan taki został po raz pierwszy ogłoszony od dnia 14 marca 2020 r.
11 Por. https://www.gov.pl/web/gov/mozesz-legalnie-przebywac-w-polsce-na-podstawie-tzw-krotkoterminowych-tytulow-pobytowych (dostęp: 18 marca 2021 r.).
12 Zob. także https://www.gov.pl/web/gov/przedluzenie-waznosci-zezwolenia-na-prace-i-oswiadczenia (dostęp: 8 kwietnia 2021 r.).

Oferty współpracy

Francja

Francuska firma poszukuje producenta blatów stołowych z włókna drzewnego. Kontrahent z Francji specjalizuje się w projektowaniu i produkcji stołów szkolnych. Firma zainteresowana jest nawiązaniem współpracy w ramach umowy podwykonawstwa z producentami blatów stołowych wykonanych z płyty pilśniowej o średniej gęstości (MDF) z zaokrąglonymi narożnikami i krawędziami. Numer referencyjny BRFR20210218001

Grecja

Grecka firma, działająca w branży sportowo-rekreacyjnej i specjalizująca się w internecie rzeczy, opracowała projekt inteligentnej kamizelki ratunkowej z funkcjami poprawiającymi bezpieczeństwo, wygodę i komunikację użytkowników sportów wodnych. Dwie główne funkcje kamizelki to system ogrzewania utrzymujący stałą temperaturę ciała użytkownika i system śledzenia w czasie rzeczywistym, który skraca czas ewentualnej akcji ratunkowej o 80–90%. Firma poszukuje partnera zdolnego wyprodukować kamizelkę według jej projektu, na podstawie umowy produkcyjnej. Numer referencyjny BRGR20200826001

Hiszpania

Hiszpańska firma, zajmująca się gazyfikacją odpadów i wytwarzaniem z nich energii, poszukuje technologii wychwytywania lub składowania CO_2 i technologii utylizacji dwutlenku węgla w celu zmniejszenia śladu węglowego procesu gazyfikacji. Firma oferuje współpracę na podstawie umowy licencyjnej, umowy handlowej z pomocą techniczną lub współpracę technologiczną. Numer referencyjny TRES20210318001

Litwa

Litewska organizacja rządowa, działająca w sektorze ochrony środowiska, poszukuje innowacyjnych rozwiązań w zakresie analizy ryzyka środowiskowego stwarzanego przez firmy w ramach prowadzonej przez nie działalności gospodarczej. Obecnie lista kontrolowanych podmiotów wraz z planem ich kontroli jest sporządzana w arkuszach kalkulacyjnych Excel. Na ich podstawie sporządzany jest roczny plan kontroli przedsiębiorstw. Jednakże z uwagi na liczbę firm w rejestrze (29 tysięcy) i ograniczone zasoby kadrowe litewska organizacja poszukuje rozwiązania, które umożliwi skuteczną selekcję firm wskazanych do kontroli, pod kątem największego zagrożenia dla środowiska. Organizacja oferuje współpracę w ramach umowy o współpracy technicznej. Numer referencyjny TRLT20210318001

Niemcy

Niemiecka firma, świadcząca szeroki wachlarz usług i indywidualnych rozwiązań z zakresu izolacji termicznej, akustycznej i przeciwpożarowej, w tym napraw i konserwacji, poszukuje pracowników doświadczonych w instalacji systemów izolacyjnych w budownictwie i przemyśle. Firma oferuje współpracę na podstawie umowy o podwykonawstwo. Numer referencyjny BRDE20210326001

Niemiecki hurtownik drewnianych artykułów dla gryzoni poszukuje partnerów w Europie. Partner z Niemiec jest w szczególności zainteresowany takimi akcesoriami dla chomików, królików czy ptaków, jak zabawki, elementy wyposażenia do budek i klatek (kryjówki, gniazda itd.). Firma oferuje umowę dostawy lub umowę produkcyjną. Numer referencyjny BRDE20210302001

Więcej ofert współpracy zagranicznej znajdą Państwo w bazie POD na stronie: www.een.org.pl (zakładka Oferty współpracy).

Rumunia

Rumuński dystrybutor z branży meblarskiej nawiąże współpracę z producentami różnych rodzajów mebli wypoczynkowych. Firma posiada ponad 10-letnie doświadczenie w detalicznej sprzedaży mebli drewnianych na terenie Rumunii, Grecji i Węgier. Poszukiwane produkty będą sprzedawane zarówno w sklepach stacjonarnych, jak i online. Numer referencyjny BRRO20210106001

Rumuński importer poszukuje dostawców profili i innych elementów konstrukcyjnych wykonanych z PCV. Zapotrzebowanie firmy obejmuje elementy o różnych wymiarach, kolorach i kształtach do produkcji okien, drzwi, okiennic itp., zarówno do wewnętrznego, jak i zewnętrznego zastosowania. Numer referencyjny BRRO20210216001

Serbia

Serbski dystrybutor poszukuje dostawców farmaceutyków i wyrobów medycznych. Firma istnieje na rynku od 26 lat i współpracuje z wieloma firmami farmaceutycznymi z całego świata: zarówno z międzynarodowymi koncernami, jak i małymi producentami. Partner z Serbii oferuje umowę dystrybucyjną. Numer referencyjny BRRS20210105001

Włochy

Włoski startup, specjalizujący się w produkcji biodegradowalnych mebli z odpadów organicznych, poszukuje partnera do produkcji płytek i ulepszenia ich procesu barwienia. Partner powinien mieć doświadczenie w branży chemicznej, które zostanie wykorzystane do analizy materiałów odpadowych użytych w procesie produkcji i barwienia płytek i będzie miał za zadanie rozwiązać problem odporności takich płytek na wilgoć. Startup oferuje współpracę na podstawie umowy o współpracy badawczej. Numer referencyjny TRIT20210330001

SOLVIT
– POMOC DLA OBYWATELI I PRZEDSIĘBIORCÓW

Spotykasz się z niewłaściwym stosowaniem prawa UE
w innych państwach Wspólnoty?
SOLVIT pomoże rozwiązać problem.

SOLVIT to międzynarodowa sieć pod auspicjami Komisji Europejskiej, obejmująca instytucje państw członkowskich Unii Europejskiej (oraz Norwegii, Lichtensteinu i Islandii), której celem jest **pomoc w rozwiązywaniu sporów z administracją publiczną** danego państwa Wspólnoty, powstałych w związku z **niewłaściwym stosowaniem prawa UE**.
SOLVIT jest umiejscowiony w Departamencie Spraw Europejskich w Ministerstwie Rozwoju, Pracy i Technologii.

Obywatele i przedsiębiorcy mogą zgłaszać do SOLVIT problemy:

- wynikające z naruszenia prawa UE z zakresu rynku wewnętrznego,
- spowodowane przez administrację innego państwa członkowskiego,
- zawierające element transgraniczny (np. obywatel danego państwa UE ma problemy z urzędem innego kraju Wspólnoty).

Jak działa SOLVIT?

- Zgłaszamy problem do Centrum SOLVIT – w ciągu tygodnia otrzymujemy odpowiedź od Centrum, czy zgłoszenie jest zasadne.
- Jeśli tak – mamy 4 tygodnie na przesłanie do Centrum materiałów świadczących o nieprawidłowym stosowaniu prawa UE przez urząd w innym kraju Wspólnoty.
- Po ocenie nadesłanych materiałów, Centrum odmawia lub przyjmuje sprawę – ma 10 tygodni na rozwiązanie problemu.

Adres kontaktowy e-mail do polskiego Centrum SOLVIT: solvit@mrpit.gov.pl

Więcej informacji na temat SOLVIT
https://www.gov.pl/web/rozwoj-praca-technologia/solvit