

Prawo a biznes – jak to pogodzić? Wybrane zagadnienia z życia firmy

W TYM WYDANIU:

Niezamówiona informacja handlowa. Przegląd orzecznictwa i dopuszczalne metody stosowania marketingu bezpośredniego

2

Compliance – problemy z polską ustawą i zgłaszanie naruszeń prawa w grupie przedsiębiorstw

8

Prasówka

11

Kary z Polski i świata

13



Olga Ograbisz

Niezamówiona informacja handlowa. Przegląd orzecznictwa i dopuszczalne metody stosowania marketingu bezpośredniego

W dynamicznym świecie konkurencji, skuteczny marketing to klucz do sukcesu. Jednak często utrudniają go liczne i często nie do końca zrozumiałe przepisy prawne.

Jak interpretować przepisy, na co zwrócić uwagę, czego na pewno się wystrzegać a co można pominąć w zakresie informacji handlowej i marketingu bezpośredniego – o tych i innych kwestiach czytajcie w tym artykule.

Informacja handlowa, której definicję wprowadza ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną to w uproszczeniu każda informacja przeznaczona do promowania towarów, usług lub wizerunku podmiotów gospodarczych działających na rynku, która służy osiągnięciu określonych efektów handlowych.

Informacja handlowa to każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy, lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niestrużących osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi.

(ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (DZ.U. z 2020 r. poz. 344))

W świetle obowiązujących obecnie przepisów prawa same w sobie informacji handlowej nie stanowią:

- informacje umożliwiające bezpośredni dostęp do działalności organizacji, w szczególności mowa tu o nazwie domeny czy adresie poczty elektronicznej,
- informacje odnoszące się do towarów, usług czy wizerunku organizacji opracowane w sposób niezależny (jeżeli są udzielane bez wzajemnych świadczeń finansowych).

Rozwijając powyższe, dane dotyczące organizacji, które służą nam nawiązaniu z nią kontaktu, w tym adresy e-mail czy witryny internetowe nie będą uznawane za informacje handlowe (chyba że mają one charakter czysto handlowy). Podobnie

w przypadku marketingu (tzw. content marketing), który nie zawiera w sobie kwestii promocyjnych czy reklamowych. Na przykład: samo zestawienie produktów danego przedsiębiorstwa nie będzie stanowić informacji handlowej w świetle obecnie obowiązujących przepisów prawa, w szczególności, jeżeli zostały przygotowane przez niezależny podmiot. Jeżeli jednak z takim zestawieniem idzie dodatkowo informacja o możliwości zamówienia konsultacji lub zakupu, wówczas traci ona swój niehandlowy charakter.

Warunki przekazywania informacji handlowej na gruncie prawa krajowego reguluje ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, która w art. 10 jasno wprowadza zakaz przesyłania niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Warunkiem zalegalizowania powyższych działań jest uzyskanie zgody odbiorcy, który świadomie i dobrowolnie udostępnił identyfikujący go adres e-mail. Podobnie sytuacja wygląda w przypadku przekazywania informacji za pośrednictwem telekomunikacyjnych urządzeń końcowych czy automatycznych systemów wywołujących, co z kolei uregulowane zostało w art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648).

Należy także podkreślić, że przekazywanie informacji handlowej zarówno poprzez wiadomość e-mail, telefonicznie, jak i za pośrednictwem innych automatycznych systemów wywołujących bez zgody osoby fizycznej stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233).

Art. 10. Zakaz przesyłania niezamówionej informacji handlowej

1. Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.
2. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny.
3. Działanie, o którym mowa w ust. 1, stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy, o której mowa w art. 9 informacja handlowa, ust. 3 pkt 1.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

Marketing bezpośredni a regulacje prawne

Ustawa Prawo telekomunikacyjne rozszerza katalog działań regulowanych o marketing bezpośredni. Definiowany jest on jako działania polegające na komunikowaniu informacji

promocyjnych do wyselekcjonowanej grupy konsumentów, w celu uzyskania bezpośredniej ich reakcji z pominięciem bezpośredniego kontaktu ze sprzedawcą/usługodawcą. Jedną z form prowadzenia marketingu bezpośredniego jest marketing internetowy, w którym wykorzystuje się Internet do prezentacji i sprzedaży produktów/usług przy pomocy różnego rodzaju narzędzi, w tym komunikatów graficznych.

Legalność prowadzenia działań o charakterze marketingu bezpośredniego, podobnie jak przesyłanie informacji handlowych należy rozważać na gruncie:

- ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (dalej u.s.u.d.e.),
- ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (dalej: ustawa Prawo telekomunikacyjne),
- ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (dalej: ustawa o ochronie konkurencji i konsumentów),
- ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny,
- 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: RODO).

Wszystkie z powyższych aktów prawnych wytyczają granice, w jakich przedsiębiorca może prowadzić swoje działania promocyjne bez uszczerbku dla praw i wolności konsumentów. RODO w motywie 47 dopuszcza możliwość prowadzenia działań marketingowych w oparciu o uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO), jednak administrator musi zapewnić możliwość wniesienia bezpłatnie i w dowolnym momencie sprzeciwu wobec takiego przetwarzania (art. 21 ust. 2 RODO, motyw 70 RODO).

Doktryna w zakresie ochrony konsumentów nakazuje natomiast bezwzględne uzyskanie zgody od osób, do których ma zostać skierowana reklama czy informacja handlowa. Zgoda ta co do zasady powinna być dobrowolna i świadoma oraz wyrażona w konkretnym, jasno zdefiniowanym celu. Brak takiej zgody, zgodnie ze stanowiskiem Urzędu Ochrony Konkurencji i Konsumentów (dalej: UOKiK), stanowi naruszenie prawa i może być podstawą do wystąpienia przez adresata marketingu z roszczeniami cywilnoprawnymi wobec nadawcy. Może być także uznana za czyn nieuczciwej konkurencji lub praktykę naruszającą zbiorowe interesy konsumentów, jak również stanowi

wykroczenie ścigane na wniosek pokrzywdzonego. Co istotne zgoda nie może być domniemana, a konsument, podążając za opinią Grupy Roboczej Art. 29, powinien mieć zapewnioną kontrolę nad własnymi danymi oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia oferowanych warunków.

Niezamówiona informacja handlowa – zmora działów marketingu

W opinii specjalistów ds. marketingu prowadzenie działań promocyjnych, wymagających zgody odbiorcy, zawsze wiąże się z pewnymi trudnościami. Odnosząc się do kwestii problemu dotyczącego wysyłania do użytkowników zapytania o zgodę na przesłanie informacji handlowej czy też wykonywania połączeń telefonicznych, należy zauważyć, że praktyka ta w świetle brzmienia art. 24 ustawy o świadczeniu usług drogą elektroniczną w zw. z art. 24 ust. 1 ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń (t.j. Dz. U. z 2010 r. Nr 46, poz. 275, z późn. zm.) może stanowić wykroczenie zagrożone grzywną w wysokości do 5000 zł, które ścigane jest na wniosek pokrzywdzonego.

W szczególności chodzi o sytuację, w której nadawca wysyła wiadomość z pytaniem, czy odbiorca wyraża zgodę na otrzymywanie informacji handlowych dotyczących określonego produktu, czy usługi i jednocześnie wraz z pytaniem przekazuje pełną lub większość informacji o oferowanych produktach, lub usługach, których pytanie dotyczy. Wiadomość taką należy uznać za niezamówioną informację handlową, ponieważ poza samym pytaniem zawiera treści promujące konkretny produkt lub usługę. Zasadność takiej interpretacji potwierdza definicja informacji handlowej zawarta w art. 2 pkt 2 ustawy o świadczeniu usług drogą elektroniczną. Kluczowe znaczenie w tym kontekście ma zamiar nadawcy polegający na osiągnięciu efektu

handlowego oraz bezpośrednia promocja towarów, usług etc.

Z drugiej natomiast strony trudno jest uznać samo pytanie zawierające dodatkowo wskazanie profilu działalności nadawcy za niezamówioną informację handlową, jeżeli sama w sobie nie zmierza do promocji produktów lub usług. W związku z tym w celu umożliwienia odbiorcy podjęcia decyzji co do wyrażenia zgody na przesłanie informacji handlowych lub jej braku wydaje się, iż powinien on dysponować co najmniej kierunkową, ogólną wiedzą na temat profilu prowadzonej przez nadawcę pytania działalności (źródło: Odpowiedź podsekretarza stanu w Ministerstwie Administracji i Cyfryzacji — z upoważnienia ministra — na interpelację nr 6350 w sprawie wysyłania wiadomości SPAM)

” Imienny adres poczty elektronicznej, w szczególności członków zarządu, nie podlega ochronie przepisów RODO, ponieważ jest on wykorzystywany w działalności osoby prawnej.

Na co warto również zwrócić uwagę podczas planowania działań o charakterze marketingowym – to do kogo tak naprawdę wiadomość jest kierowana. W zdaniu drugim motywu 14 RODO regulator wprost wskazał, że RODO nie dotyczy przetwarzania danych osobowych, dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. Istotą sprawy jest zatem ocena czy adres imienny poczty elektronicznej, którym dysponujemy, należy zakwalifikować do katalogu danych osobowych, o których mowa w art. 4 pkt 1 RODO czy nie.

Sąd Administracyjny (II SA/WA 559/22) w jednym ze swoich postanowień wskazuje jasno, że imienny adres poczty elektronicznej, w szczególności członków zarządu, nie podlega ochronie przepisów RODO, ponieważ jest on wykorzystywany w działalności osoby prawnej. Co więcej, zgodnie z wyrokiem SA/Wa 3310/21 istnieje możliwość zgodnego z prawem oparcia przetwarzania ogólnie dostępnych danych osobowych, w celu prowadzenia działań marketingowych na prawnie uzasadnionym interesie administratora, pomimo braku związania administratora z podmiotem danych wcześniejszym



relacjami gospodarczymi lub biznesowymi. Takie dopuszczenie jest możliwe, jeżeli adres e-mail odbiorcy wiadomości został publicznie wskazany np. w serwisie internetowym z zachęceniem do kontaktu.

Podsumowując, możliwe jest przesyłanie informacji handlowej oraz podejmowanie działań marketingowych bez uprzedniej zgody odbiorcy, jeżeli działania te skierowane są do osób prawnych lub reprezentantów osób prawnych, których dane kontaktowe wykorzystywane są w działalności osoby prawnej. Nie dotyczy to jednak osób prowadzących jednoosobowe działalności gospodarcze. Te w świetle obowiązującego prawa krajowego uznawane są za osoby fizyczne i w związku z tym podlegają ochronie m.in. na gruncie RODO.

Niezamówiona informacja handlowa i działania marketingowe – wybrane orzecznictwo

Biorąc pod lupę krajowe i międzynarodowe orzecznictwo w zakresie niezgodnych z prawem działań w obszarze marketingu bezpośredniego oraz przesyłania niezamówionej informacji handlowej można wysunąć następujące wnioski:

- większość kar została nałożona za naruszenie zbiorowych interesów konsumentów,
- kary głównie nakładane są przez instytucje działające w obronie interesów konsumentów w tym UOKiK oraz UKE,
- główną przyczyną złamania prawa było podejmowanie działań marketingowych bez uprzedniej zgody użytkownika końcowego, odbiorcy.

**Jak prowadzić działania marketingowe, zgodne z RODO?
Kliknij i sprawdź!**

Poniżej przedstawiamy zestawienie najbardziej medialnych postępowań z ostatnich kilku lat, które odnoszą się do braku respektowania praw i wolności osób fizycznych w obszarze marketingu bezpośredniego.

1. NETIA SA – decyzja UOKiK nr DOZIK 3/2019 (Warszawa dn. 30 maja 2019 r.) – podmiot prowadził praktyki naruszające zbiorowe interesy konsumentów polegające na wykonywaniu połączeń telefonicznych do konsumentów niebędących abonentami Spółki, których dane pozyskane zostały od partnerów Spółki, w celu marketingu bezpośredniego oferty Spółki (nakłanianie do zawarcia umowy) pomimo nieudzielenia przez tych konsumentów uprzedniej zgody. Zgodę próbowano uzyskać podczas rozmowy telefonicznej, co również zostało uznane za niezgodne z prawem.

Decyzja: Netia uniknęła kary finansowej, ponieważ zobowiązała się do zmiany dotychczasowych praktyk, w tym zasad współpracy ze swoimi partnerami oraz zobowiązania ich nie tylko do uzyskania zgód zgodnie z obowiązującym prawem, ale również przekazania ich do Netii. Ponadto zaproponowała osobom poszkodowanym różnego rodzaju rekompensaty od finansowych po oferty umów na preferencyjnych warunkach.

Link do decyzji.

2. ACS MEDICA – decyzja UOKiK nr RPZ 14/2018 (Poznań, 21 grudnia 2018 r.) – podmiot prowadził praktyki, naruszające zbiorowe interesy konsumentów, polegające m.in. na wykonywaniu połączeń telefonicznych do konsumentów dla celów marketingu bezpośredniego, pomimo braku uprzednich zgód konsumentów na ww. działania. Działania marketingowe głównie polegały na kierowaniu telefonicznych zaproszeń na organizowane przez przedsiębiorcę pokazy handlowe.

Decyzja: kara pieniężna w wysokości 6 467,00 zł

Link do decyzji.

3. ARSTELE – Decyzja nr RPZ 9/2019 (13 września 2019 r.) oraz Wyrok XVII AmA 37/19 Sąd Okręgowy w Warszawie – przedmiotem postępowania prowadzonego wobec podmiotów było naruszenie zbiorowych interesów konsumentów poprzez błędną wykładnię przepisów prawa, w tym zbyt szeroką interpretację pojęcia marketingu bezpośredniego i bezpodstawne uznanie, że wyłączona jest możliwość jakiegokolwiek kontaktu z abonentem

bez jego uprzedniej zgody, jeśli choćby pośrednim skutkiem takiego kontaktu miałyby być zawarcie umowy, w tym w szczególności wyłączona jest możliwość nawiązania połączenia dla uzyskania zgody na kontakt w celu marketingu bezpośredniego.

Sąd podtrzymał stanowisko UOKiK, w obszarze interpretacji pojęcia zgody uprzedniej. Idąc za organami, nie można uznać zgody na prowadzenie działań związanych z marketingiem bezpośrednim za uprzednią, jeżeli pytanie o nią zostało postawione na początku rozmowy, której celem są ww. działania. Nawet jeśli zostanie ona udzielona, to już po użyciu numeru telefonu użytkownika i zakłóceniu jego wolności od otrzymywania niezamówionej informacji handlowej.

Decyzja: kara finansowa w wysokości 69 967,00 zł

[Link do decyzji.](#)

4. Koksztys S.A. – Decyzja UKE z 18 czerwca 2019 r. – podmiot naruszył przepisy art. 172 ust. 1 oraz art. 174 ustawy Prawo telekomunikacyjne poprzez niewypełnienie obowiązku uzyskania uprzedniej zgody na używanie telekomunikacyjnych urządzeń końcowych do celów marketingu bezpośredniego i użycie tych urządzeń do nawiązania 30 636 kontaktów telefonicznych, w celu poinformowania o działalności Koksztys, w tym promowaniu usług w zakresie umów abonamentowych na usługi prawne i windykacyjne. Mówiąc dokładniej, przedsiębiorstwo zleciło wykonywanie telefonicznych połączeń o charakterze marketingowym, nie posiadając wymaganych prawem zgód abonentów lub użytkowników końcowych.

Decyzja: kara finansowa w wysokości 80 000, 00 zł (przy czym pod uwagę wzięto to, że podmiot nie był dotychczas karany przez Prezesa UKE)

[Link do decyzji.](#)

5. Telecom Media S.A. – Decyzja UOKiK nr DDK 11/2011 (Warszawa 30 grudnia 2011 r.) – przedsiębiorstwo naruszyło zbiorowe interesy konsumentów m.in. poprzez wykonywanie połączeń głosowych oraz wysyłanie krótkich wiadomości tekstowych (SMS), nakłaniających konsumentów do wzięcia udziału w konkursie bez

uprzedniej zgody tychże konsumentów. W opinii Prezesa prowadzone działania stanowią także agresywną praktykę rynkową, o której mowa w art. 9 pkt 3 ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym.

Decyzja: kara finansowa w wysokości 18 851,00 zł

[Link do decyzji.](#)

6. Smak i Zdrowie Sp. z o.o. – decyzja UOKiK nr DOZiK 1/2019 (Warszawa marzec 2019) – organizacja naruszyła zbiorowe interesy konsumentów poprzez wykorzystanie telekomunikacyjnych urządzeń końcowych dla celów marketingu bezpośredniego dotyczącego produktów podmiotu bez uprzedniej zgody abonentów lub użytkowników końcowych.

Decyzja: kara finansowa w wysokości 35 388,00 zł

[Link do decyzji.](#)

7. Orange Polska S.A. – decyzja UKE (13 listopada 2018 r.) – Spółka naruszyła przepisy prawa poprzez wykorzystywanie automatycznych systemów wywołujących do celów marketingu bezpośredniego, nie wykazując posiadania wymaganych zgód abonentów lub użytkowników końcowych. Skala procederu objęła łącznie 3 820 185 numerów telefonów abonentów lub użytkowników końcowych. Orange podjęło jednak działania zmierzające do zadośćuczynienia ww. osobom za bezprawne rozesłanie wiadomości SMS poprzez przyznanie im specjalnych bonusów (pakietów danych) – stanowiło to jeden z czynników łagodzących przy ustalaniu wysokości kary.

Decyzja: kara finansowa w wysokości 9,1 mln zł

[Link do decyzji.](#)

8. Acc Consulting Varsinais-Suomi - Fiński organ właściwy ds. ochrony danych osobowych (Tietosuojaalutuetun Toimisto), a bardziej precyzyjnie – Rada ds. sankcji tego organu – nałożył administracyjną karę pieniężną na fińską spółkę organizującą szkolenia. Regulator zarzucił ukaranemu administratorowi, że ten prowadził działania o charakterze

marketingowym bez stosownej zgody oraz nie respektował praw osób, których dane dotyczą, w tym nie realizował ich żądań, kierowanych na podstawie przepisów RODO. W toku postępowania Spółka wskazywała, że wiadomości reklamowe kierowane były bezpośrednio do kontrahentów, tj. prawdopodobnie osób prawnych, a baza danych subskrybentów utworzona została z bazy danych osób kontaktowych (uprawnionych do reprezentacji kontrahenta). Zgodnie z fińskimi przepisami krajowymi (kodeks społeczeństwa informacyjnego) uprzednia zgoda na marketing bezpośredni nie jest wymagana. Regulator nie podzielił jednak tego stanowiska i nałożył karę finansową za wysyłkę materiałów marketingowych bez zgody osób fizycznych oraz za niezrealizowanie praw podmiotów danych tj. usunięcia danych i wycofania zgody.

Decyzja: kara finansowa w wysokości 7000 euro (niecałe 32 000 zł)

Kilka praktycznych porad w zakresie marketingu bezpośredniego od LexDigital

1. Zanim podejmiesz konkretne działania marketingowe, upewnij się, kto jest ich odbiorcą i czy posiadasz odpowiednie zgody tych osób – sprawdź nie tylko cel, dla którego zgoda została wyrażona, ale również kanał komunikacji.
2. Współpracujesz z podmiotami zewnętrznymi, które w Twoim imieniu wykonują marketing – zadбай o odpowiednio skonstruowane umowy i zobowiązań podwykonawcę do pozyskiwania zgód w Twoim imieniu. Proś o potwierdzenie.
3. Dysponujesz bazą zawierającą liczne dane kontaktowe do osób (obecni, byli czy potencjalni klienci, etc.), którym chcesz przedstawić informacje handlowe związane z Twoją działalnością, ale nie posiadasz wymaganych zgód – zaplanuj działania zgodnie z zasadą dwóch rozmów – podczas pierwszej odpytaj o zgodę na kontakt; podczas drugiej przedstaw ofertę o ile podczas pierwszej rozmowy ta zgoda została udzielona.
4. Rozmowa, podczas której pozyskujemy zgodę, powinna zawierać obowiązek informacyjny. Dobrze byłoby, aby była ona nagrywana, aby zachować rozliczalność oraz móc bez obaw przedstawić dowody na pozyskanie zgody spełniające wymogi prawa w razie kontroli UODO, UOKiK czy innych organów. Fakt udzielenia lub nie zgody powinien być także odnotowany w bazie, lub powinny być tworzone dwie bazy – osób, które wyraziły zgodę i odrębnie tych, co jej nie wyrazili.

Na co warto zwrócić uwagę – we wszystkich powyżej wskazanych przypadkach czynnikiem zdecydowanie łagodzącym wysokość kary były działania podejmowane przez administratorów, dążące do zadośćuczynienia poszkodowanym oraz mające na celu wyeliminowanie złych praktyk. Ponadto każda kara administracyjna miała pełnić funkcję represyjną, stanowiąc sankcję i dolegliwość za naruszenie ustawy o ochronie konkurencji i konsumentów oraz prewencyjną, zapobiegającą ponownemu naruszeniu. Podkreślano również walor wychowawczy, odstraszaający dla innych organizacji

przed stosowaniem w przyszłości tego typu praktyk w obrocie z konsumentami.

A na koniec..

Na podstawie wyżej wskazanych przypadków kar/upomnień/decyzji organów innych niż Urząd Ochrony Danych Osobowych, uznać należy, że stosowanie marketingu bezpośredniego z wykorzystaniem numeru telefonu lub adresu e-mail przekazanego organizacji w celach innych, niż działania marketingowe, obarczone jest wysokim ryzykiem, w tym ryzykiem nałożenia na daną organizację administracyjnych kar pieniężnych.

Podczas gdy RODO dopuszcza stosowanie marketingu bezpośredniego na podstawie prawnie usprawiedliwionego interesu administratora (w szczególności wobec osób, które w jakimś stopniu mogą spodziewać się takich działań, ze względu na ich powiązanie z administratorem), tak inne regulacje bezdyskusyjnie wymagają uzyskania jednoznacznych i uprzednich zgód na wykorzystanie konkretnych kanałów komunikacji za pośrednictwem, których taki marketing ma być świadczony. Przekazywanie niezamówionej informacji handlowej może być również uznane za czyn nieuczciwej konkurencji i podlegać karze grzywny. Należy także zwrócić uwagę, że nawet jeżeli kara finansowa nie będzie dotkliwa, to nadszarpnięta zostanie renoma i wizerunek organizacji, która podejmie takie ryzyko, a to z kolei może przełożyć się na potencjalne przyszłe zyski.

LexDigital odradza swoim klientom szeroko zakrojone działania marketingowe, kiedy istnieje chociaż cień ryzyka naruszenia przepisów obowiązującego prawa, w szczególności w zakresie posiadania odpowiednich zgód. Niemniej mając na uwadze reguły rynku i gospodarki oraz różny apetyt organizacji na ryzyko najbardziej bezpiecznym rozwiązaniem jest zastosowanie „zgody uprzedniej”, a więc wykonanie połączenia w celu uzyskania zgody, a następnie kolejnego w celu przedstawienia oferty (to samo dotyczy się korespondencji mailowej). Pamiętając przy tym, że pierwsza wiadomość musi być wolna od jakichkolwiek informacji, co do których istnieje nawet cień podejrzenia, że mogą służyć reklamie danego organizacji i jej produktów czy usług.



Jakub Pawłowski

Compliance – problemy z polską ustawą o sygnalistach i zgłaszanie naruszeń prawa w grupie przedsiębiorstw

Niebawem, bo już 17 grudnia 2023 r. minie ostateczny termin wdrożenia przez Polskę przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (dalej jako „Dyrektywa”). Polska nadal nie uchwaliła przepisów implementujących Dyrektywę, a dotychczasowe wysiłki w tym zakresie niestety zamiast rozjaśniać ten obszar wprowadzają jeszcze więcej wątpliwości. Ochrona sygnalistów nadal zatem czeka na uregulowanie.

Termin wdrożenia

Wspomniana na wstępie data 17 grudnia 2023 r. dotyczy wyłącznie – i to na drodze wyjątku – wdrożenia przepisów regulujących zgłaszanie naruszeń prawa w organizacjach z sektora prywatnego, zatrudniających od 50 do 249 pracowników. Dyrektywa reguluje jednak również sektor publiczny, a w tym przypadku termin implementacji dyrektywy już dawno upłynął (dokładnie 17 grudnia 2021 r.)

Niezależnie od tego, o którym sektorze mowa, można kolokwialnie powiedzieć, że Polska jest daleko w lesie z implementacją. Począwszy od października 2021 r., a skończywszy na lipcu br. w ramach prac

Rządowego Centrum Legislacyjnego, powstało bowiem aż 8 różnych projektów ustawy o ochronie osób zgłaszających naruszenia prawa. Ostatni projekt datowany na 12 lipca 2023 r. (dalej jako „**Projekt ustawy**”) nadal nie trafił do Sejmu i trudno w jakikolwiek sposób przewidywać, kiedy projekt trafi do pod obrady.

Kto jest zobowiązany do wdrożenia?

Dyrektywy unijne są specyficznym aktem prawnym. W przeciwieństwie do chociażby do rozporządzeń unijnych, nie są stosowane bezpośrednio w każdym państwie członkowskim, lecz poprzez implementację. Co do zasady, adresatami norm zawartych w dyrektywach są bowiem państwa członkowskie, które są zobowiązane do przyjęcia odpowiednich przepisów lokalnych wypełniających cel dyrektywy. Dopiero przyjęte przez państwo członkowskie przepisy formalnie kreują obowiązki i prawa wobec jednostek.

Są jednak sytuacje, w których dyrektywa może znaleźć bezpośrednie zastosowanie. Taka sytuacja może mieć miejsce, gdy:

1. przepisy dyrektywy są wystarczająco precyzyjne i bezwarunkowe,
2. ich stosowanie nie jest uzależnione od dalszych

działań ze strony instytucji unijnych lub organów państw członkowskich,

3. z norm dyrektywy wynikają prawa jednostek wobec państwa, tj. skierowane są one na przyznanie praw jednostkom,
4. upłynął termin implementacji dyrektywy przez dane państwo członkowskie albo implementacja jest nieprawidłowa.

Dowiedz się kim jest sygnalista, kiedy się nim zostaje i jakie normy prawne go chronią. Kliknij i przeczytaj nasz artykuł!

Co istotne, na bezpośredni skutek dyrektywy można się powołać wyłącznie przeciwko państwu (ewentualnie przeciwko podmiotom z sektora publicznego stanowiącym emanację państwa). Innymi słowy, jednostka (np. osoba fizyczna) nie może się powołać na przepisy niewdrożonej dyrektywy przeciwko innej jednostce (np. spółce).

Co to wszystko oznacza dla podmiotów i organizacji działających w Polsce?

Podmioty z sektora prywatnego teoretycznie mogą czekać na przyjęcie polskich przepisów. Nie ma bowiem żadnego ryzyka powołania się przeciwko takim podmiotom bezpośrednio na przepisy dyrektywy.

Co innego w przypadku podmiotów z sektora publicznego. W przypadku tych podmiotów, termin implementacji dyrektywy już minął i tutaj w niektórych przypadkach może zachodzić ryzyko bezpośredniego stosowania dyrektywy.

Czy wdrażać system zgłaszania naruszeń pomimo braku ustawy?

Wdrożenie systemu przyjmowania zgłoszeń aktualnie jest problematyczne, głównie przez dużą niepewność co do kształtu przepisów. Jest jednak kilka argumentów, które przemawiają za przyjęciem odpowiednich rozwiązań jeszcze przed uchwaleniem nowych przepisów.

Przede wszystkim, dotychczasowy Projekt ustawy przewiduje krótki okres *vacatio legis*. Ustawa ma bowiem wejść w życie po upływie 2 miesięcy od dnia ogłoszenia, przy czym przepisy dotyczące przyjmowania zgłoszeń wewnętrznych (czyli zgłoszeń przyjmowanych wewnątrz organizacji) miałyby wejść już po 14 dniach. To bardzo krótki czas na zorganizowanie całego systemu przyjmowania zgłoszeń, na który składa się wiele elementów, począwszy od wyboru kanału zgłoszeń, opracowania procedury przyjmowania zgłoszeń, a skończywszy na wyborze i przeszkoleniu osób odpowiedzialnych za przyjmowanie zgłoszeń. Nie można również zapominać o tym, że przyjmowanie zgłoszeń i ochrona sygnalistów, to spore wyzwanie na gruncie ochrony danych osobowych, gdzie konieczna jest analiza skutków dla ochrony danych, prawidłowa realizacja obowiązków informacyjnych.

Oprócz kwestii ściśle prawnych za wdrożeniem systemu przyjmowania zgłoszeń od sygnalistów przemawiają również względy wizerunkowe i etyczne. Poprawnie funkcjonujący system przyjmowania zgłoszeń pozwala na szybsze identyfikowanie nieprawidłowości lub nadużyć w organizacji.

Wdrożenie systemu przyjmowania zgłoszeń w grupie przedsiębiorstw

Sygnalistą jest osoba, która zgłasza wewnątrz organizacji lub na zewnątrz (organom ścigania lub podmiotom nadzorującym) naruszenia norm prawnych, o których dowiedziała się w związku z wykonywaniem obowiązków zawodowych w zakładzie pracy.

Dyrektywa parlamentu europejskiego i rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia aktów legislacyjnych Unii posługuje się pojęciem „osoba dokonująca zgłoszenia”, które oznacza osobę fizyczną, która zgłasza lub ujawnia publicznie informacje na temat naruszeń, uzyskane w kontekście związanym z wykonywaną przez nią pracą.

Zgodnie z aktualnym brzmieniem Projektu ustawy podmioty zatrudniające co najmniej 50 osób będą zobowiązane wdrożyć procedurę zgłoszeń wewnętrznych. Wyjątkiem będą podmioty m.in. wykonujące działalność w zakresie usług, produktów i rynków finansowych oraz przeciwdziałania praniu

pieniędzy i finansowaniu terroryzmu, bezpieczeństwa transportu i ochrony środowiska – takie podmioty będą zobowiązane do wdrożenia systemu niezależnie od pułapu zatrudnienia.

Podstawowym obowiązkiem każdego podmiotu wdrażającego system obsługi zgłoszeń sygnalistów będzie ustalenie wewnętrznej procedury zgłaszania naruszeń prawa, która będzie wskazywała wewnętrzną jednostkę organizacyjną lub osobę w ramach struktury organizacyjnej podmiotu prawnego, lub podmiot zewnętrzny, upoważnione przez podmiot prawny do przyjmowania zgłoszeń.

Projekt ustawy, w ślad za Dyrektywą, przewiduje jednocześnie możliwość wspólnego ustalenia zasad, dotyczących przyjmowania i weryfikacji zgłoszeń oraz prowadzenia postępowania wyjaśniającego przez podmioty prywatne, na rzecz których wykonuje pracę co najmniej 50, lecz nie więcej niż 249 osób. Co jednak istotne, takie podmioty mają być odrębnymi administratorami pozyskanych w związku z przyjmowaniem i weryfikacją zgłoszeń danych osobowych i jako odrębni administratorzy nie mają wzajemnie dostępu do danych, pozyskanych przez odrębnego administratora.

Powyższe założenia są dyskusyjne co najmniej z dwóch względów.

Po pierwsze, oznacza to, że największe podmioty z sektora prywatnego, tj. zatrudniające powyżej 249 osób, które jednocześnie np. są powiązane kapitałowo z innym podmiotem (np. spółką-córką) nie będą mogły współdzielić zasobów służących przyjmowaniu zgłoszeń od sygnalistów. Tak skonstruowane przepisy mogą prowadzić do sytuacji, w której grupa przedsiębiorstw nie będzie mogła wprowadzić jednego systemu przyjmowania zgłoszeń.

Po drugie, zapisy Projektu ustawy dotyczące odrębnego administrowania danymi osobowymi przez podmioty współdzielące zasoby sprawiają,

że praktycznie niemożliwe będzie tworzenie w ramach grupy przedsiębiorstw jednej jednostki odpowiedzialnej za przyjmowanie i rozpatrywanie zgłoszeń. Skutkiem takiej regulacji będzie możliwość jedynie współdzielenia kanału zgłoszeń (np. platformy whistleblowingowej), ale z zachowaniem pełnej odrębności co do danych, a to w praktyce będzie utrudniało sprawne przyjmowanie zgłoszeń. Co więcej, taki kształt przepisów będzie oznaczał konieczność większego zaangażowania osób biorących udział w wyjaśnianiu zgłoszeń.

” Projekt ustawy przewiduje krótki okres vacatio legis. Ustawa ma bowiem wejść w życie po upływie 2 miesięcy od dnia ogłoszenia, przy czym przepisy dotyczące przyjmowania zgłoszeń wewnętrznych miałyby wejść już po 14 dniach.

Problem z zewnętrznymi podmiotami

Zgodnie z Projektem ustawy procedura zgłoszeń wewnętrznych powinna określać bezstronną, wewnętrzną jednostkę organizacyjną lub osobę w ramach struktury organizacyjnej podmiotu prawnego, upoważnione do podejmowania działań następczych. Zadaniem takiej jednostki lub osoby będzie m.in. podjęcie działań w celu oceny prawdziwości informacji zawartych w zgłoszeniu, w szczególności przez postępowanie wyjaśniające. Będą one upoważnione do weryfikacji zgłoszenia i dalszej komunikacji ze zgłaszającym, w tym występowania o dodatkowe informacje i przekazywania zgłaszającemu informacji zwrotnej.

Powyższą rolę wg Projektu ustawy będzie mogła pełnić wewnętrzna jednostka organizacyjna lub osoba upoważniona do przyjmowania zgłoszeń, jeżeli zapewnia ona bezstronność. Projektowany przepis pomija natomiast podmioty zewnętrzne, a to oznacza, że np. kancelarie prawne albo spółka matka w przypadku grupy przedsiębiorstw nie będą mogły prowadzić postępowania wyjaśniającego. Może się to okazać sporym utrudnieniem w prowadzeniu postępowań wyjaśniających, bowiem nie wszystkie organizacje będą dysponowały odpowiednimi zasobami.





Prasówka



Koniec nielegalnego nagrywania rozmów pracowników i klientów w znanych aptekach. Rzecznik Praw Obywatelskich bada sprawę

W jednej z większych sieci aptek w Polsce nagrywano pracowników oraz klientów przy okienkach. Osoby pracujące podpisywali zgody, klienci zaś nic nie wiedzieli.

Portal "Puls Farmacji" ujawnił szereg skarg od farmaceutów, techników farmaceutycznych oraz byłych lub obecnych pracowników tej sieci aptek. Była pracownica opowiedziała, że podczas podpisywania umowy o pracę została poproszona o podpisanie zgód na rejestrowanie obrazu i dźwięku. Jednak dostała tylko kopię umowy o pracę. O tym, gdzie zamontowane są mikrofony, dowiedziała się od innych pracowników. Kierownictwo nie wyjaśniło powodów nagrywania ani przeznaczenia nagrań.

Nikt z pracowników, nawet farmaceuci i kierownicy aptek, nie mieli dostępu do nagrań z kamer i mikrofonów. Co kilka tygodni każdy pracownik otrzymywał ocenę oraz wytyczne od koordynatora, kładące nacisk na sprzedaż zamienników, wydawanie leków w mniejszych opakowaniach oraz marek własnych.

Sprawa podważa prawo do prywatności objęte konstytucyjnymi gwarancjami (art. 47 Konstytucji RP). Dodatkowo problem ten może wpłynąć na prawa pracowników wynikające z Kodeksu pracy (art. 22 [2] Kp), zezwalające na nadzór nad terenem zakładu pracy dla zapewnienia bezpieczeństwa i ochrony mienia. Rzecznik pyta prezes Naczelnej Rady Aptekarskiej, czy podjęto działania w celu

wyjaśnienia sprawy i czy skontaktowano się z odpowiednimi instytucjami, takimi jak Urząd Ochrony Danych Osobowych oraz Państwową Inspekcją Pracy.

Źródło: <https://bit.ly/3MUMWKP>

EROD blokuje przetwarzanie danych osobowych na potrzeby reklamy behawioralnej przez Meta

27 października EROD podjęła pilną wiążącą decyzję, zobowiązując irlandzki organ nadzoru, jako główny organ nadzorczy do podjęcia ostatecznych środków dotyczących Meta oraz do nałożenia zakazu przetwarzania danych osobowych na potrzeby reklamy behawioralnej w całym Europejskim Obszarze Gospodarczym na podstawie prawnej umowy i uzasadnionego interesu.

Decyzja ta wynika z wniosku norweskiego Organu Ochrony Danych o podjęcie ostatecznych środków w tej sprawie. Zakaz przetwarzania danych na potrzeby reklamy behawioralnej wejdzie w życie po tygodniu od powiadomienia administratora o ostatecznych środkach przez IE SA. Meta została powiadomiona o tej decyzji w dniu 31 października.

EROD bada propozycję Meta opartą na zgodzie jako podstawie prawnej, ale ostateczna decyzja zapadnie po wspólnej ocenie zainteresowanych organów nadzoru. Przewodnicząca EROD podkreśliła, że konieczne jest zakończenie nielegalnego przetwarzania danych przez Meta i dostosowanie się do przepisów dotyczących ochrony danych osobowych.

Źródło: <https://bit.ly/49sRnWP>

Niemiecki sąd orzeka: właściciele samochodów muszą ujawnić tożsamość kierowcy zgodnie z RODO

Niemiecki sąd orzekł, że właściciel samochodu musi ujawnić tożsamość kierowcy w celu ścigania wykroczeń drogowych, zgodnie z art. 6 ust. 1 lit. f Rozporządzenia o Ochronie Danych Osobowych (RODO). Administratorem w tej sprawie była firma, której pracownicy korzystali z pojazdów firmowych. Po popełnieniu wykroczeń drogowych nie ustalono, kto kierował pojazdem. Władze publiczne poprosiły o ujawnienie tożsamości kierowcy i nakazały prowadzenie rejestru pojazdów oraz osób, które miały dostęp do nich, co było uzasadnione niemieckim prawem o ruchu drogowym.



Administrator odmówił i złożył apelację, argumentując, że RODO zabrania ujawniania danych osobowych kierowców władzom oraz prowadzenia rejestru z ich nazwiskami. Sąd apelacyjny jednak podtrzymał wyrok pierwszej instancji, uznał, że ujawnienie danych i prowadzenie rejestru są dozwolone na podstawie RODO, opierając się na ochronie uzasadnionych interesów organów w wykonywaniu zadań w interesie publicznym, w tym w ściganiu naruszeń przepisów administracyjnych. Ponadto sąd stwierdził, że dalsze etapy przetwarzania danych są zgodne z przepisami władz publicznych na podstawie art. 6 ust. 1 lit. e RODO. To orzeczenie ma wpływ na kwestię ochrony danych osobowych w przypadku naruszeń prawa drogowego.

Źródło: <https://bit.ly/3MyDDzX>

Próby ułatwienia swobodnego przepływu danych z Chin

Chiny mają zamiar ułatwić międzynarodowym korporacjom (MNC) przestrzeganie przepisów dotyczących eksportu danych z Chin. Planują to osiągnąć, umożliwiając rutynowe eksportowanie danych związanych z codzienną działalnością biznesową i zarządzaniem zasobami ludzkimi oraz eksport niewielkich ilości nieistotnych danych, co zwolni z konieczności stosowania trzech podstawowych mechanizmów zgodności w eksportowaniu danych.

Chińska Administracja Cyberprzestrzeni (CAC) opublikowała projekt przepisów regulujących transgraniczny przepływ danych. MNC często przenoszą dane osobowe zasobów ludzkich do innych krajów w celu zarządzania nimi poza Chinami. Aby uniknąć konieczności stosowania trzech mechanizmów, konieczne jest ustanowienie prawnie uzasadnionej polityki zarządzania zasobami ludzkimi lub umowy zbiorowej. To stanowi podstawę prawną do eksportu danych osobowych pracowników w celach zarządzania zasobami ludzkimi.

MNC powinny monitorować i identyfikować dane klasyfikowane jako "ważne dane" oraz dokładnie dokumentować pochodzenie zebranych danych, zwłaszcza tych pozyskanych poza Chinami. Warto zauważyć, że nawet w przypadku spełnienia zasad safe harbor, nadal wymagana jest zgoda osób, których dane dotyczą, do przesyłania danych osobowych z Chin, zgodnie z przepisami PIPL (Personal Information Protection Law - chiński odpowiednik RODO). Dlatego MNC muszą przeprowadzać analizę skutków przetwarzania danych (PIA) jako środek zgodności.

Źródło: <https://bit.ly/3sk6T6D>

Chcesz dowiedzieć się więcej o chinskiej umowie o transgranicznym przekazywaniu danych osobowych? Kliknij i przeczytaj nasz artykuł



Polska

Wojewódzki Sąd Administracyjny w Warszawie utrzymał karę finansową nałożoną na Virgin Mobile (obecnie P4) za naruszenie przepisów RODO. Wcześniej Urząd Ochrony Danych Osobowych obniżył karę z 1,9 mln zł na 1,6 mln zł, ale decyzja Prezesa UODO została utrzymana przez sąd. Sąd uznał, że administrator nie wprowadził odpowiednich środków technicznych i organizacyjnych do zapewnienia bezpieczeństwa danych osobowych, co doprowadziło do naruszenia zasad ochrony danych. Sąd uznał także, że kara była prawidłowo ustalona i uzasadniona, a P4 przejęło wszystkie obowiązki Virgin Mobile, w tym odpowiedzialność za naruszenia przepisów RODO.

Źródło: <https://bit.ly/45XEmS9>

Świat

Hellenic Data Protection Authority (HDPa) nałożył grzywnę w wysokości 50 000 euro na organizację transportu miejskiego w Atenach (OASA) za naruszenie przepisów RODO. OASA naruszył zasadę ograniczenia przechowywania danych, gdyż przechowywał dane osobowe swoich klientów przez 20 lat bez wyjaśnienia konieczności tego działania. Ponadto naruszył art. 35 ust. 1 RODO, ponieważ jego ocena skutków dla ochrony danych była niewystarczająca i nieokreślona w kwestii celów przechowywania danych oraz ryzyka związanego z przetwarzaniem.

HDPa nakazał OASA wprowadzenie zmian w swoim systemie oraz dokonanie identyfikacji i udokumentowania okresów przechowywania danych do różnych celów przetwarzania. Ponadto OASA musi poprawić swoją ocenę skutków dla ochrony danych w ciągu trzech miesięcy.

Źródło: <https://bit.ly/45XEuB7>

Szwedzki organ ochrony danych nałożył karę w wysokości 800 000 SEK (około 68 324 EUR) na Radę Edukacji w Sztokholmie za naruszenie

przepisów RODO związanych z monitoringiem w szkole Aspudden. Monitoring obejmował znaczny obszar szkoły i nie został dostatecznie uzasadniony, naruszając przepisy dotyczące przetwarzania danych osobowych. Ponadto, brak dostarczenia klarownych informacji uczniom, opiekunom i pracownikom oraz niepełne oznakowanie kamer stanowiły dodatkowe naruszenia zasad RODO. Organ ochrony danych nałożył karę administracyjną i nakazał poprawienie informacji na stronie internetowej miasta Sztokholm w ciągu czterech tygodni.

To naruszenie miało znaczenie ze względu na fakt, że przetwarzanie danych obejmowało dzieci objęte obowiązkiem uczęszczania do szkoły oraz pracowników. Karę nałożono na Radę Edukacji za brak zgodności z przepisami dotyczącymi przejrzystości i uczciwości wobec osób, których dane były przetwarzane, a także za naruszenie zasady minimalizacji danych.

Źródło: <https://bit.ly/40zptnR>

Francuski organ ochrony danych nałożył karę w wysokości 600 000 euro na GROUPE CANAL+ w związku z 31 skargami dotyczącymi naruszenia przepisów RODO. Skargi dotyczyły "zimnych" połączeń telefonicznych oraz problemów z wykonywaniem praw przez osoby, których dane były przetwarzane. Firma nie uzyskała ważnej zgody na "zimne" połączenia, naruszyła zasady przejrzystości i naruszyła obowiązek powiadomienia DPA o poważnym naruszeniu danych osobowych w 2020 roku.

Ponadto, organ ochrony danych uznał, że firma nie przestrzegała obowiązków wynikających z prawa konsumentów, nie informując potencjalnych klientów o celu przetwarzania danych podczas "zimnych" połączeń. Dodatkowo, firma nie wywiązała się z zobowiązań dotyczących składanych przez klientów wniosków o usunięcie danych oraz prawo do sprzeciwu wobec przetwarzania, co również doprowadziło do naruszenia przepisów RODO. Sankcja została nałożona na firmę w związku z naruszeniem przepisów RODO i przepisów krajowych.

Źródło: <https://bit.ly/40tJ4Wn>

Chorwacki organ ochrony danych nałożył grzywnę w wysokości 25 000 EUR na Zagrebački Holding D. o. o. za naruszenie art. 13 RODO i art. 25 ust. 2 RODO. Zagrebački Holding D. o. o. jest spółką publiczną, będącą własnością miasta Zagrzeb, oferującą usługi publiczne, w tym komunalne, zaopatrzenie w wodę i odwodnienie, dystrybucję gazu i usługi rynkowe. Firma poprosiła osoby korzystające z jej usług o dostarczenie kopii dowodu osobistego w celu otrzymania kopii rachunku za pośrednictwem poczty elektronicznej, co zostało uznane za naruszenie RODO.

Podczas dochodzenia, chorwacki organ ochrony danych stwierdził, że firma nie posiadała określonego

regulaminu wewnętrznego w celu identyfikacji użytkowników żądających dostarczenia kopii faktury za pośrednictwem poczty elektronicznej, co naruszało przepisy dotyczące odpowiednich środków technicznych i organizacyjnych. Dodatkowo, firma nie poinformowała użytkowników o podstawie prawnej przetwarzania i okresie przechowywania danych osobowych podczas zbierania kopii ich dokumentów identyfikacyjnych, naruszając przepisy dotyczące informacji o przetwarzaniu danych. W wyniku tych naruszeń, firma otrzymała grzywnę w wysokości 25 000 euro.

Źródło: <https://bit.ly/3FNRnTz>

Newsletter RODO

Październik 2023 nr 3/2023

Dziękujemy za przeczytanie naszego Newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI

P.S. Czy wiesz, że...

wg Tableau 63% konsumentów na całym świecie uważa, że firmy nie są uczciwe co do tego, w jaki sposób wykorzystują ich dane osobowe, a prawie 48% konsumentów przestało kupować od firm z powodu obaw o prywatność.

