Szymon Ciach

PRAWO W IT

PRAKTYCZNIE I PO LUDZKU

onepress Helion

Redaktor prowadzący: Wojciech Ciuraj
Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *https://onepress.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://onepress.pl/user/opinie/prapol
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-8532-0

Printed in Poland.

SPIS TREŚCI

Część 3. Technologie a prawo

Część 4. Regulacje IT

Część 5. Spory i transakcje M&A w IT

ROZDZIAŁ 16.

REGULACJE IT — PRZEGLĄD WYBRANYCH

W tej części znajduje się omówienie wybranych regulacji. Zostało ograniczone do aktów prawnych, które najlepiej w ocenie autora obrazują ogólne trendy.

Wiele tych regulacji już jest (lub po wejściu w życie będzie) obszarem głębokiej specjalizacji. Od kilku lat obserwujemy skutki obowiązywania RODO, w wyniku którego wzrosło zapotrzebowanie na ekspertów w tej dziedzinie. Dogłębne omówienie jednej tego typu regulacji to pozycja o potencjalnej objętości kilkuset stron, niewątpliwie więc regulacje IT są bardzo atrakcyjną dziedziną dla badań naukowych. W wyniku dynamicznego ich rozwoju pojawia się potrzeba stworzenia przekrojowego ujęcia tych regulacji.

Regulacje przetwarzania i ochrony danych

Aktów prawnych na tym polu przybywa. Historycznie były to raczej regulacje wertykalne (sektor finansowy, medyczny, publiczny etc.). W ostatnich latach rozwijają się regulacje horyzontalne, których kamieniem milowym UE było RODO.

RODO

Rozporządzenie Parlamentu Europejskiego i Rady nr 2016/679 to unijne rozporządzenie o ochronie danych osobowych. Jego głównymi celami są ujednolicenie przepisów dotyczących ochrony danych w państwach Unii, a także ochrona prywatności i wzmocnienie praw osób fizycznych.

Dane osób fizycznych korzystających z rozwiązań cyfrowych od lat są przetwarzane na masową skalę. Z jednej strony niesie to zagrożenie dla prywatności osób fizycznych, a z drugiej jest elementem gospodarki cyfrowej. W internecie podstawową walutą obok pieniądza stały się dane użytkowników. Wiele usług i treści dostępnych w sieci bez dodatkowej opłaty bazuje na tym, że uda się zebrać dane na temat użytkowników, a następnie zaprezentować im odpowiednie reklamy. Rzeczywiście zatem następuje tu pewien cyfrowy barter, co zdaje się być coraz wyraźniej dostrzegane przez regulatorów[1].

Podstawowe założenia. Przede wszystkim każdej osobie fizycznej przysługuje zestaw praw do jej danych osobowych, np. prawo do żądania zaprzestania ich przetwarzania (prawo do bycia zapomnianym).

[1] Zob. *https://www.gamingtechlaw.com/2021/04/facebook-not-free-personal-data-italian-court/*, dostęp 17.11.2023.

Oczywiście od tych praw przysługują wyjątki, bo w praktyce niemożliwe lub społecznie nieuzasadnione byłoby realizowanie takich uprawnień w każdej sytuacji. Przykładowo: dłużnik mógłby sabotować ewentualne dochodzenie należności, żądając od kontrahenta usunięcia wszystkich jego danych.

Ponieważ dane są pewnym aktywem osoby fizycznej, ogólna reguła jest taka, że w Unii zakazane jest ich przetwarzanie. Dopiero wyjątki od tej zasady pozwalają podmiotom gospodarczym przetwarzać dane, stanowiąc tzw. podstawy prawne przetwarzania danych osobowych. Taką podstawą prawną jest np. zgoda osoby fizycznej.

Wiekopomność RODO zaznacza się również w zastosowaniu na ogromną skalę **podejścia opartego na analizie ryzyka**. W ramach RODO nastąpiło odejście od sztywnych wskazań procedur i zabezpieczeń, jakie należy wdrożyć (tzw. *checklisty*). W to miejsce pozostawiono podmiotom dużo swobody w doborze środków służących ochronie danych osobowych, „proporcjonalnych" do ryzyk i działalności podmiotu. Podejście oparte na analizie ryzyka często jest wykorzystywane w kolejnych unijnych regulacjach IT. Ma ono swoje zalety — pozwala tworzyć regulacje stosunkowo neutralne technologicznie i mające potencjał do przetrwania próby czasu w dynamicznym świecie IT. Wadą jest zdecydowanie mniejszy komfort prawny podmiotów regulowanych. Same muszą podejmować konkretne decyzje co do środków bezpieczeństwa i nigdy nie mogą być pewne, czy organ nadzoru *post factum* nie oceni sytuacji niekorzystnie. Taka regulacja daje dużą władzę organom nadzoru. Odmienna ocena może się wiązać z nałożeniem kary. To jest ostatnie z kluczowych założeń RODO — duże kary mierzone nie w kwotach, lecz procentach od obrotu, stały się etatowym narzędziem legislacji unijnej w zakresie regulacji IT.

Adresaci. RODO jest skierowane do nieograniczonego grona podmiotów, przy czym w praktyce dla podlegania pod RODO znaczenie mają podstawowe definicje, np. definicja przetwarzania danych. Na podstawie wyraźnych wyłączeń RODO nie stosuje się do niektórych sytuacji, w tym do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze (np. zebranie listy gości na imprezę urodzinową). RODO przewiduje dwie wspomniane już główne role dla swoich adresatów: administrator danych osobowych i podmiot przetwarzający. Trudności w praktyce szczególnie rodzą sytuacje, gdzie w ramach jednej współpracy jedna ze stron lub obie realizują jednocześnie obydwie te role. Może to dotyczyć tych samych lub różnych zakresów informacji, co zostało szerzej omówione w rozdziale 10., „Umowy dotyczące zasobów IT".

Zagadnienia. Oprócz tego, że RODO wzmacnia prawa osób fizycznych, jego przepisy przede wszystkim dotyczą przetwarzania danych przez przedsiębiorców. W momencie wejścia w życie wprowadziło równe warunki prawne działania dla firm w UE, które wcześniej znacznie różniły się w poszczególnych państwach członkowskich. Z perspektywy organizacji międzynarodowych dalej występują lokalne różnice, choćby w podejściu organów nadzoru, jednakże fundament przepisów jest wspólny. Firmy przetwarzające dane w dużej skali musiały powołać jednostki (inspektorów ochrony danych) odpowiedzialne za ochronę danych. W niektórych przypadkach wprowadzono obowiązek analizowania, jak kolejne projekty i rozwiązania wpływają na ochronę danych, co stało się elementem procesu zakupu nowych technologii. Wreszcie ustanowiono obowiązek raportowania incydentów związanych z przetwarzaniem danych osobowych.

RODO jest dla współczesnych regulacji danych w Unii Europejskiej swoistym punktem odniesienia. Stanowi również wzór dla zagranicznych regulacji ochrony danych osobowych[2].

Dane nieosobowe

Niedługo po rozpoczęciu stosowania RODO (maj 2018 r.) uchwalono ***Rozporządzenie 2018/1807 ws. ram swobodnego przepływu danych nieosobowych w UE***[3]. To jeden z pierwszych kroków w stronę systemu prawnego danych nieosobowych, domykającego otwarte pole *data economy* pozostawione przez RODO.

Podstawowym elementem tego aktu prawnego jest zakaz nakładania przez państwa członkowskie wymogów dotyczących lokalizacji danych, chyba że są one uzasadnione względami bezpieczeństwa publicznego. Innymi słowy: państwa UE nie mogą prowadzić polityki protekcjonizmu w zakresie danych, wymuszającej korzystanie z lokalnych centrów przetwarzania danych. Sam fakt istnienia tego rozporządzenia wskazuje na trend traktowania ogólnie rozumianych danych jako cennego aktywa. Trend ten przejawia się zwłaszcza w dwóch kolejnych regulacjach: *Data Governance Act* i *Data Act*. Wspólnie będą stanowić trzon regulacji danych nieosobowych.

[2] Na przykład prawo stanu Kalifornia, zob. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557964*, dostęp 17.11.2023.

[3] *https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32018R1807*, dostęp 26.01.2024.

Data Governance Act

Data Governance Act **(DGA)**[4] to *Rozporządzenie 2022/868 w sprawie europejskiego zarządzania danymi* (**akt w sprawie zarządzania danymi**). DGA jest elementem polityki unijnej budowania gospodarki opartej na danych poprzez tworzenie tzw. **europejskich przestrzeni danych**.

W uproszczeniu idea ta polega na narzucaniu określonym podmiotom obowiązków w zakresie odpowiedniego przygotowania danych i umożliwienia do nich dostępu innym podmiotom. Dostęp odbywa się w zakresie i na zasadach opisanych regulacją, może być ograniczony dla podmiotów spełniających określone warunki (np. posiadających zezwolenie). Jedną z pierwszych implementacji tego pomysłu była **dyrektywa PSD 2**[5], która zmusiła banki do udostępniania danych innym podmiotom (tzw. *open banking*). Trwają prace legislacyjne nad rozszerzeniem tego modelu na inne branże sektora finansowego (np. ubezpieczenia) w ramach tzw. **rozporządzenia FIDA**[6].

Data Governance Act to regulacja, której jednym z głównych celów jest zapewnienie łatwiejszego dostępu do danych będących w posiadaniu podmiotów sektora publicznego. Część tych danych może być chroniona (np. prawami własności intelektualnej), a więc w tradycyjnych warunkach prawnych ich wykorzystanie musiałoby się odbywać głównie

[4] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724* (akt w sprawie zarządzania danymi).

[5] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego*.

[6] Zob. projekt rozporządzenia FIDA, tj. wniosek *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) 1095/2010 i (UE) 2022/2554*, COM/2023/360 final.

na bazie umów. Potrzebna była zatem standaryzacja zasad na poziomie unijnym, tak by dostęp do tych danych był prostszy i spójny w całej Unii. W ramach DGA określono warunki dostępu i wykorzystywania tych danych, np. dopuszczalne przypadki dostępności danych na wyłączność i pobieranie opłat. W celu dalszego pogłębiania współpracy podmiotów sektora publicznego ustanowiono też Europejską Radę ds. Innowacji w zakresie Danych.

W rozporządzeniu DGA wprowadzono nową kategorię usług regulowanych, tj. **usługi pośrednictwa danych**. Podmiot, który chce prowadzić taką działalność, musi wpisać się do odpowiedniego rejestru i przestrzegać zasad działalności opisanych w DGA. Otrzymuje status **dostawcy usług pośrednictwa danych** (ang. *data intermediation services provider*, **DISP**). Uzasadnienie wprowadzenia tej regulacji wynika z tego, że firmy niechętnie dzielą się danymi z obawy przed niewłaściwym ich wykorzystaniem lub utratą przewagi konkurencyjnej[7]. Uregulowanie DISP ma zapewnić, że podmioty te będą funkcjonować jako godni zaufania pośrednicy, co powinno zachęcić firmy do wymiany danych, przy jednoczesnym zachowaniu kontroli nad tymi danymi. Ponadto DISP mogą pośredniczyć w obrocie danymi między osobami fizycznymi a firmami.

Generalny kierunek regulacyjny jest więc taki, aby osoba, której dotyczą dane, zarówno osobowe, jak i nieosobowe, miała możliwość udostępnienia tych danych (w tym odpłatnego) za pośrednictwem zaufanego podmiotu. Dziś użytkownik stron internetowych i produktów z elementem cyfrowym jest traktowany dość przedmiotowo. Korzystając z usług cyfrowych, generuje dane na swój temat, które są przetwarzane i monetyzowane na różne sposoby przez dostawców tych

[7] *https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained*, dostęp 18.11.2023.

usług. Użytkownik zaś często nie ma dostępu do tych danych (poza danymi osobowymi) i nie partycypuje w „ekonomii" danych, które go dotyczą. Regulacje danych mają użytkownika „upodmiotowić" w tym zakresie, a działalność DISP ma być jednym ze służących do tego narzędzi.

Działalność DISP można podzielić na trzy kategorie:

- **Usługi pośrednictwa między posiadaczami danych a potencjalnymi użytkownikami danych** — np. *data marketplace'y* (**rynki danych**), czyli portale internetowe oferujące dostęp do danych od różnych podmiotów umożliwiający tym podmiotom zarabianie na obrocie danymi, które od nich pochodzą[8].
- **Usługi pośrednictwa między osobami, których dane dotyczą, zamierzającymi udostępnić swoje dane osobowe lub dane nieosobowe, a potencjalnymi użytkownikami danych** — chodzi o to, aby osoba mogła wystawić swoje dane na sprzedaż za pomocą takich usług, a także zarządzać tymi danymi poprzez wykonywanie swoich uprawnień wynikających z RODO (np. zgłoszenie żądania zaprzestania przetwarzania danych osobowych).
- **Usługi świadczone przez spółdzielnie danych** — swoisty odpowiednik organizacji zbiorowego zarządzania prawami w zakresie danych osobowych i nieosobowych, działający na rzecz swoich członków, zarówno firm i osób fizycznych; obejmuje np. organizacje zbiorowego udostępniania danych.

Przykładami usług pośrednictwa danych są także pule danych (ang. *data pools*), tworzone wspólnie przez grupę osób prawnych lub fizycznych z zamiarem udzielania licencji na korzystanie z danych wszystkim zainteresowanym stronom. Za usługi pośrednictwa danych nie są zasadniczo

[8] Na przykład *https://dih.telekom.com/en*, dostęp 26.01.2024.

uznawane usługi przechowywania w chmurze, usługi analityczne, dostarczanie oprogramowania na potrzeby dzielenia się danymi, przeglądarki internetowe, wtyczki do przeglądarek, poczta elektroniczna[9].

W ramach DGA ustanowiono również ramy prawne tzw. **altruizmu danych**, czyli dobrowolnego dzielenia się danymi, bez wynagrodzenia wykraczającego poza zwrot kosztów, realizowanego w celach leżących w interesie ogólnym — opieka zdrowotna, zapobieganie zmianie klimatu, poprawa mobilności etc. W tym celu stworzono nową kategorię organizacji *non profit*, tj. uznanych organizacji altruizmu danych. Ich działalność jest uregulowana w DGA i ma wspierać dobrowolne dzielenie się danymi.

Data Act

***Data Act* (akt w sprawie danych)**[10], tj. rozporządzenie dotyczące sprawiedliwego dostępu do danych i ich wykorzystywania, w chwili pisania tej książki jest jeszcze w fazie prac legislacyjnych. Jeśli jednak podstawowe założenia tej regulacji się nie zmienią, już dziś może być określona mianem RODO dla IoT[11].

[9] Jeżeli usługi takie dostarczają jedynie narzędzia techniczne osobom, których dane dotyczą, lub posiadaczom danych, to celem dostarczania takich narzędzi nie jest nawiązywanie stosunków handlowych między posiadaczami danych a użytkownikami danych.

[10] Wniosek *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania* (akt w sprawie danych), COM(2022) 68 final, 2022/0047(COD).

[11] Internet rzeczy odnosi się do rozwiązań opartych na generowaniu i wymianie danych z różnego rodzaju urządzeniami (domowymi, codziennego użytku, transportu etc.).

Regulacja ta dopełnia system prawny europejskiej gospodarki danych, którego już obowiązującymi fundamentami są RODO i *Data Governance Act*. RODO dotyczy tylko jednej kategorii danych (dane osobowe), a *Data Governance Act* otwiera dane sektora publicznego i wprowadza ramy prawne dla usług pośrednictwa danych. Celem *Data Act* jest zaś **uregulowanie zasad przetwarzania i prowadzenia biznesu na danych nieosobowych** pochodzących z tzw. urządzeń skomunikowanych.

Data Act w dużej mierze jest przeznaczony dla rynku związanego z internetem rzeczy (ang. *Internet of Things*, IoT). Dziś wiele urządzeń, w tym przemysłowych, medycznych, transportowych, jak i codziennego użytku, jest podłączonych do sieci (np.: urządzenia kuchenne, zegarki, urządzenia *smart home*). Urządzenia te zbierają i przesyłają dane do producenta, który dzięki tym danym może rozwijać swoje produkty, a także w inny sposób zarabiać na ich analizie i dalszym udostępnianiu. Podmiot, którego dane dotyczą, jak wspominano, zasadniczo nie bierze czynnego udziału w ekonomii danych generowanych przy jego udziale. Ponadto podmiot, najczęściej producent urządzenia, który zbiera te dane, nie ma prawnego obowiązku dzielić się nimi z innymi podmiotami, zwłaszcza konkurencją. Kupując „tradycyjny" produkt, nabywa się wszystkie jego części i akcesoria. Jednak w przypadku zakupu produktu skomunikowanego, który generuje dane, często nie jest jasne, kto i co może z tymi danymi zrobić. *Data Act* ma uregulować te sytuacje — ułatwić użytkownikom łatwiejsze przenoszenie ich danych i określić, kto może tworzyć wartość z tych danych i na jakich warunkach[12].

Podstawowe założenia *Data Act* są takie, że osoba, która korzysta z urządzenia, generując dane, i której takie dane dotyczą, powinna mieć pewne prawa wobec tych danych, a firma, która te dane zbiera, powinna

[12] *https://digital-strategy.ec.europa.eu/en/policies/data-act*, dostęp 19.11.2023.

się nimi podzielić z rynkiem. W konsekwencji użytkownik powinien stać się aktywnym graczem na rynku obejmującym dane generowane przy jego współudziale. W przestrzeni całej gospodarki regulacja ma (w założeniu) przeciwdziałać zdobywaniu nadmiernej pozycji rynkowej przez podmioty kontrolujące dane z IoT.

Żeby osiągnąć powyższe cele, w *Data Act* zdefiniowano wiele podstawowych pojęć, począwszy od **produktu skomunikowanego** odnoszącego się do urządzeń przetwarzających dane i **powiązanej usługi** jako kluczowego elementu cyfrowego danego produktu, wpływającego na korzystanie z jego funkcji oraz na przekazywanie danych. Określono również kategorie podmiotów uczestniczących w rynku danych z IoT. Kształt definicji jeszcze nie jest ostateczny, jednak prace zmierzają w kierunku ustanowienia następujących ról i obowiązków:

- **użytkownik danych** — tj. podmiot, który ma zgodny z prawem dostęp do danych i ma prawo do wykorzystywania tych danych w celach komercyjnych lub niekomercyjnych;
- **posiadacz danych** — tj. podmiot, który uzyskał dostęp do danych lub wygenerował dane z produktu skomunikowanego lub usługi powiązanej (np. producent urządzenia); będzie miał obowiązek m.in. udostępnienia danych użytkownikowi i odbiorcy;
- **odbiorca danych** — tj. podmiot, inny niż użytkownik produktu skomunikowanego lub powiązanej usługi, który może zwrócić się do posiadacza danych o udostępnienie danych. Może to być np. konkurencyjny producent urządzeń.

Rynek danych z IoT w kształcie wynikającym z *Data Act* będzie oparty w dużej mierze na prawnych obowiązkach poszczególnych aktorów. Niektóre budzą kontrowersje, szczególnie wpływ obowiązku udostępnienia danych na ochronę tajemnicy przedsiębiorstwa. Obowiązki te będą istotne w całym cyklu życia produktu skomunikowanego. Od

producentów tych produktów wymagane będzie projektowanie produktów w taki sposób, by umożliwić uprawnionym podmiotom dostęp do danych generowanych przez taki produkt. Wymogi *Data Act* będą musiały zatem zostać uwzględnione przez producentów już we wczesnej fazie prac analitycznych (np. odpowiednie formaty i struktura danych, możliwość ich eksportu). Kiedy już dane zostaną wygenerowane, podmiot, który je „zbiera", czyli posiadacz danych, będzie musiał udostępnić je kilku rodzajom podmiotów: (i) osobom, których dane dotyczą, (ii) użytkownikom, (iii) odbiorcom danych na wniosek użytkownika lub osoby, której dane dotyczą, (iv) podmiotom publicznym (w pewnych przypadkach).

Podczas realizowania obowiązku udostępnienia danych może wystąpić wiele przeszkód (np. nieakceptowalne warunki umowne, wysokie opłaty). W ramach *Data Act* narzucone zatem będą pewne minimalne standardy w zakresie warunków umownych o udostępnianiu danych, w tym dość szczegółowe regulacje dla „rozsądnego" wynagrodzenia, jakiego mogą żądać posiadacze danych od odbiorców danych.

O ile udostępnienie danych użytkownikowi przez posiadacza musi się odbywać nieodpłatnie, o tyle użytkownik będzie mógł te dane dalej udostępnić już odpłatnie (np. na rynku danych uregulowanym w ramach DGA).

Przewiduje się również wymogi dla dostawców usług przetwarzania danych (dostawcy hostingu, chmury obliczeniowej etc.). Mają one przeciwdziałać zjawisku uzależnienia zamawiającego od dostawcy takiej usługi (tzw. *vendor lock-in*) i ułatwiać klientom zmianę dostawcy tych usług. Wprowadzone będą również zasady żądania dostępu do danych przez podmioty sektora publicznego, a także ramy prawne dla norm i wspólnych specyfikacji w zakresie interoperacyjności danych.

W ramach *Data Act* uwzględniono, że dane generowane przez produkt skomunikowany lub usługę powiązaną mogą obejmować zarówno dane osobowe, jak i nieosobowe. W zakresie danych osobowych jasno stwierdzono, że zastosowanie znajdują przepisy RODO i to one mają pierwszeństwo w razie kolizji. Udostępnienie danych osobowych może się więc odbywać jedynie na podstawie odpowiedniej podstawy prawnej, szczególnie zgody użytkownika. W praktyce będzie to wymagało budowania rozwiązań uwzględniających podział przetwarzanych danych co najmniej na osobowe i nieosobowe. Możliwość realizacji praw wynikających z RODO przez osobę fizyczną musi być zachowana również w modelach biznesowych opartych na *Data Act*.

Rozporządzenie ePrivacy

Rozporządzenie *ePrivacy* (**rozporządzenie w sprawie prywatności i łączności elektronicznej**)[13]. Choć pierwotny projekt został zaprezentowany już w 2017 r., w chwili pisania tej książki (listopad 2023 r.) negocjacje jeszcze trwają. Celem rozporządzenia *ePrivacy* jest zapewnienie szczegółowych zasad prywatności i ochrony danych w odniesieniu do komunikacji elektronicznej.

Najważniejsze założenia proponowanego rozporządzenia obejmują regulację tzw. dostawców usług łączności elektronicznej ***over the top*** (OTT), takich jak dostawcy usług komunikacji elektronicznej, np.: VoIP, elektroniczne komunikatory i usługi wideokonferencji. Tego typu usługi, rosnące na popularności, mają dążyć do zachowania podobnego

[13] Wniosek *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE* (rozporządzenie w sprawie prywatności i łączności elektronicznej), 2017/0003(COD).

poziomu ochrony poufności komunikacji jak tradycyjne usługi telekomunikacyjne. W szczególności obejmuje to zasady dotyczące korzystania z metadanych komunikacji, zaktualizowane zasady dotyczące plików cookie, a także objęcie komunikacji OTT zakazem spamu. Rozporządzenie ma też wzmocnić nadzór, powierzając egzekwowanie przepisów organom odpowiedzialnym za nadzorowanie zgodności z RODO.

Wprowadzenie w życie *ePrivacy* będzie miało istotny wpływ na internetowy rynek reklamy, w szczególności opartej na wiadomościach elektronicznych. Dostawcy usług OTT będą również podlegali pod ściślejsze regulacje.

Regulacje cyberbezpieczeństwa

System dyrektyw NIS

Dyrektywa NIS[14], **dyrektywa NIS 2**[15] oraz **ustawa o krajowym systemie cyberbezpieczeństwa** (**UKSC**)[16]. Wymienione akty prawne stanowią fundament regulacji w zakresie cyberbezpieczeństwa.

[14] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.*

[15] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148* (dyrektywa NIS 2).

[16] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018, poz. 1560).

Dyrektywa NIS zobowiązała państwa członkowskie do przygotowania przepisów krajowych wdrażających krajowe systemy cyberbezpieczeństwa, oparte na wspólnych standardach klasyfikacji podmiotów i ich obowiązków. Objęła także ramy współpracy w zakresie zapobiegania skutkom incydentów cyberbezpieczeństwa i ich zwalczania oraz wyznaczenia organów nadzoru. W chwili pisania tej książki (listopad 2023 r.) w życie weszła już nowsza wersja dyrektywy, tj. dyrektywa NIS 2, której termin implementacji do krajowego porządku minie w październiku 2024 r.

Ustawa o krajowym systemie cyberbezpieczeństwa (**UKSC**) stanowi krajową implementację przepisów dyrektywy NIS. Ustawa ta, oprócz ustanowienia zasad działania organów państwa, precyzuje, które podmioty wchodzą w skład krajowego systemu cyberbezpieczeństwa i tym samym podlegają pod wymogi ustawy. Oczywiście niepraktyczne byłoby nałożenie tak daleko idących wymogów w sposób horyzontalny (na wszystkich przedsiębiorców), stąd wzorem dyrektywy wymogi ustawy są kierowane do podmiotów, które mają istotne znaczenie dla gospodarki i bezpieczeństwa.

Aby podlegać pod wymogi ustawy, podmioty te muszą spełniać warunki do uznania ich za (i) **dostawców usług cyfrowych** lub za (ii) **operatorów usług kluczowych**.

Dostawcy usług cyfrowych to dość wąski zakres podmiotów, bo obejmujący tylko trzy rodzaje usług: internetowe platformy handlowe, usługi przetwarzania w chmurze, wyszukiwarki internetowe. Dostawca takich usług ma obowiązek stosować się do UKSC, co stwierdza na podstawie własnej oceny.

Operatorzy usług kluczowych to podmioty wyznaczane w drodze decyzji administracyjnej odpowiedniego organu spośród podmiotów prowadzących działalności wymienione w załączniku nr 1 do ustawy.

Rodzaje tych działalności mieszczą się w kluczowych sektorach gospodarki, takich jak energia, transport, bankowość i infrastruktura rynków finansowych oraz ochrona zdrowia.

Podmiot podlegający pod UKSC ma obowiązek wdrożyć **system cyberbezpieczeństwa** w swojej organizacji, obejmujący ustanowienie i realizowanie odpowiednich procedur ochrony bezpieczeństwa informacji. Obowiązki dotyczą m.in.: wdrożenia właściwych zabezpieczeń, wyznaczenia odpowiedzialnych osób, monitorowania systemów informacyjnych, identyfikowania podatności, testowania, identyfikowania, raportowania incydentów bezpieczeństwa i zarządzania nimi. Katalog obowiązków zależy od rodzaju podmiotu, a bardziej zaawansowane wymagania dotyczą operatora usługi kluczowej.

Dyrektywa NIS 2 nowelizuje powyższe zasady, opierając się na kilkuletnim doświadczeniu wynikającym z praktyki działania pierwszej dyrektywy i krajowych implementacji. Stanowi też odpowiedź na stale zwiększające się cyberzagrożenia. W ramach nowej dyrektywy istotnie zwiększono listę sektorów, branż i obszarów działalności gospodarczej objętych regulacjami cyberbezpieczeństwa. Dotyczy to w szczególności sektora produkcji, gospodarowania odpadami i zarządzania usługami ICT.

Podział na dostawców usług cyfrowych i operatorów usług kluczowych został uznany za nieprzydatny, w związku z czym zmieniono klasyfikację podmiotów na **kluczowe** oraz **ważne**. Podmioty świadczące usługi kluczowe to w szczególności te, które przekraczają pułap dla średnich przedsiębiorstw i prowadzą działalność w obszarze wymienionym w załączniku nr I do dyrektywy. Zalicza się do nich również niektóre podmioty sektora publicznego. Listę sektorów sklasyfikowanych jako kluczowe i ważne zawierają załączniki I i II do dyrektywy. Nowy system kwalifikacji podmiotów jest dość skomplikowany, wobec czego

w praktyce wiele podmiotów może mieć problem z jednoznacznym ustaleniem swojego statusu. Dotyczy to zwłaszcza branż, dla których wymogi w zakresie technologii informacyjnych będą stanowiły swego rodzaju *novum*.

W odniesieniu do wymogów w ramach dyrektywy NIS 2 ujednolicono wymogi dla podmiotów kluczowych i ważnych, a ich pozycja różni się zasadniczo tylko w zakresie środków nadzoru i kar. Same wymogi zaś doprecyzowano i nieco zaostrzono. W szczególności poszerzono wymagania w zakresie środków zarządzania ryzykiem w cyberbezpieczeństwie. Przyjęte przez podmiot środki zarządzania tym ryzykiem będą musiały być zatwierdzone przez organy zarządzające danego podmiotu. Organ taki będzie mógł zostać pociągnięty do odpowiedzialności za ewentualne naruszenia. Ustalono również bardziej szczegółowe wytyczne dla kar pieniężnych, jakie mogą być nakładane na podmioty kluczowe i ważne.

Dyrektywa RCE

Dyrektywa w sprawie odporności podmiotów krytycznych (*Resilience of Critical Entities*, RCE)[17] poświęcona jest zmniejszeniu podatności na zagrożenia i wzmocnieniu fizycznej odporności podmiotów krytycznych w Unii Europejskiej. O ile więc NIS 2 skupia się na sferze cyfrowej (cyberbezpieczeństwie), o tyle RCE jest jej odpowiednikiem dla sfery materialnej.

Celem wymogów zawartych w tej dyrektywie jest zapewnienie nieprzerwanego świadczenia usług kluczowych dla gospodarki i społeczeństwa

[17] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE*.

poprzez zwiększenie odporności podmiotów krytycznych świadczących te usługi. Potencjalne podmioty krytyczne to podmioty działające w takich sektorach, jak np.: energia, transport, bankowość, zdrowie oraz infrastruktura cyfrowa. Względem poprzednio obowiązujących regulacji (dyrektywa 2008/114/WE) poszerzono zakres regulowanych sektorów.

Z perspektywy IT sfera materialna jest równie istotna jak cyberbezpieczeństwo. Oprogramowanie do działania potrzebuje infrastruktury, która w wielu przypadkach jest zapewniana przez operatorów centrów przetwarzania danych, takich jak dostawcy usług chmurowych. Dlatego w katalogu **infrastruktura cyfrowa** znajdują się dostawcy punktów wymiany ruchu internetowego, dostawcy usług DNS, rejestry nazw domen najwyższego poziomu, dostawcy usług chmurowych, dostawcy usług przetwarzania danych, dostawcy sieci dostarczania treści/danych/zawartości, dostawcy usług zaufania, dostawcy publicznych sieci łączności elektronicznej, dostawcy usług łączności elektronicznej. Dostawcy tych usług będą mogli podlegać jednocześnie pod dyrektywę NIS 2 i dyrektywę RCE.

Dyrektywa będzie musiała być wdrożona i egzekwowana przez państwa członkowskie na poziomie krajowym. Będą one musiały dokonać analizy ryzyka, uwzględniając sektorowe oceny ryzyka, i na tej podstawie wskazać podmioty krytyczne. Podmioty krytyczne będą zaś miały obowiązek ochrony infrastruktury niezbędnej do utrzymania usług kluczowych (**infrastruktura krytyczna**). W przypadku naruszeń na podmiot krytyczny będą mogły być nakładane kary administracyjne.

Z dyrektywą RCE wiąże się też istotny aspekt finansowania. Państwa członkowskie będą mogły wspierać finansowo podmioty krytyczne — np. w utrzymaniu świadczenia usługi kluczowej, nawet jeśli stanie się

ona nieopłacalna dla podmiotu[18]. Wsparcie takie nie będzie traktowane jako niedozwolona pomoc publiczna.

Cybersecurity Act

***Cybersecurity Act*, tj. akt o cyberbezpieczeństwie**[19], ma na celu osiągnięcie wysokiego poziomu cyberbezpieczeństwa, cyberodporności i zaufania w UE poprzez reorganizację i wzmocnienie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz poprzez ustalenie ram prawnych dla dobrowolnych europejskich programów certyfikacji cyberbezpieczeństwa.

Ramy prawne certyfikacji tworzą system regulujący wydawanie **europejskich certyfikatów cyberbezpieczeństwa** i deklaracji zgodności z normami bezpieczeństwa dotyczącymi produktów, usług i procesów w zakresie technologii informacyjno-komunikacyjnych (ICT). Przedsiębiorcy dostarczający produkty cyfrowe w UE mogą wprowadzać je na rynek ze specjalnym oznaczeniem, jako spełniające unijne standardy cyberbezpieczeństwa. Certyfikaty te zastępują podobne programy krajowe, przy czym certyfikaty wydane w ramach takich programów krajowych obowiązują do końca ich terminu ważności. W pierwszym etapie certyfikacja jest dobrowolna, natomiast Komisja Europejska ma rozważyć uczynienie jej obowiązkową.

---

[18] Zob. *https://energetyka24.com/gaz/analizy-i-komentarze/rewolucja-w-infra*
↪*strukturze-krytycznej-w-zycie-wchodzi-ultrawazna-dyrektywa-analiza*, dostęp 19.11.2023.

[19] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013* (akt o cyberbezpieczeństwie).

Cyber Resilience Act

Akt o cyberodporności (*Cyber Resilience Act*, CRA)[20] łatwo można pomylić z aktem o cyberbezpieczeństwie, jednakże to dwie odrębne regulacje. Akt o cyberodporności w momencie pisania książki jest jeszcze na etapie procesu legislacyjnego. Jego celem jest ustanowienie standardów cyberbezpieczeństwa dla produktów z elementami cyfrowymi, czyli szeroko rozumianych urządzeń podłączonych do internetu.

Punktem wyjścia dla tej regulacji jest fakt, że coraz więcej urządzeń korzysta z oprogramowania i łączy się poprzez internet z innymi urządzeniami. Na przykładzie domowego sprzętu RTV można zauważyć, że nowoczesne urządzenia (np. telewizory, zestawy hi-fi zintegrowane z aplikacjami muzycznymi) bardzo często są zaopatrzone w systemy operacyjne i zestawy aplikacji. Nie ma jednak przepisów, które jasno regulowałyby odpowiedzialność za bezpieczeństwo oprogramowania zainstalowanego na tych urządzeniach, innego niż oprogramowanie wbudowane. Dotyczy to w szczególności utrzymania i łatania podatności cyberbezpieczeństwa. Z perspektywy użytkownika występuje zaś problem związany z posiadaniem urządzeń, które są podłączone do sieci, a mogą mieć poważne luki bezpieczeństwa. Łączy się to z problemem braku transparencji co do odpowiedzialności za poszczególne elementy produktu, w szczególności oprogramowanie.

CRA może budzić skojarzenia z *Data Act*, w którym tłem również są urządzenia zawierające oprogramowanie. **O ile w *Data Act* ustala się zasady dla biznesu na danych z IoT, o tyle w CRA chodzi o ustalenie standardów cyberbezpieczeństwa dla takich produktów.**

[20] Wniosek *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020*, COM(2022) 454 final, 2022/0272(COD).

W celu osiągnięcia powyższych założeń w ramach CRA ustalone będą zasady, które muszą zostać spełnione, aby produkt mógł być udostępniony na rynku UE. Wyróżnia się poszczególne rodzaje produktów, takie jak produkty z elementami cyfrowymi, produkty krytyczne z elementami cyfrowymi, systemy sztucznej inteligencji wysokiego ryzyka, produkty maszynowe. Na producentów takich produktów nakładane są obowiązki w zakresie cyberbezpieczeństwa, w szczególności:

- uwzględnienia wymagań cyberbezpieczeństwa na etapie projektowania produktów;
- zapewnienia, że przez przewidywany okres użytkowania produktu lub przez pięć lat po wprowadzeniu go na rynek podatności na zagrożenia będą skutecznie usuwane;
- posiadania odpowiednich procedur w zakresie cyberbezpieczeństwa, w tym obejmujących zgłaszanie zidentyfikowanych luk w produkcie lub usłudze do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA);
- zapewnienia, żeby do produktów z elementami cyfrowymi dołączano informacje i instrukcje umożliwiające ich bezpieczną instalację i użytkowanie.

W ramach CRA ustanowione mają być też obowiązki i ograniczenia dla innych podmiotów w łańcuchu dostaw. Importerzy produktów z elementem cyfrowym będą mogli wprowadzać do obrotu wyłącznie produkty, które spełniają odpowiednie wymogi. Będą mieli także obowiązek m.in. dołączenia do produktu powyższych instrukcji obsługi oraz informacji. Dystrybutorzy tych produktów przed ich udostępnieniem na rynku będą zaś sprawdzali, czy są one opatrzone oznakowaniem CE, a producent i importer wypełnili obowiązki określone w CRA.

Przewidziano też specjalne reguły na wypadek modyfikacji produktu w toku dostawy. Importer lub dystrybutor uważany jest za producenta

i podlega obowiązkom producenta, jeśli wprowadza produkt do obrotu pod własną nazwą lub znakiem towarowym albo dokonuje istotnej modyfikacji produktu już wprowadzonego. Podobnie podmiot inny niż producent, importer lub dystrybutor, jeśli dokonuje istotnej modyfikacji produktu, na potrzeby CRA uważany jest za jego producenta. Ma to na celu uporządkowanie odpowiedzialności za cyberbezpieczeństwo produktu z elementem cyfrowym w całym cyklu jego życia, a także zapewnienie odpowiedniej transparencji wobec użytkownika.

Rozporządzenie DORA

DORA (*Digital Operational Resilience Act*)[21], tj. **rozporządzenie ds. cyfrowej odporności operacyjnej sektora finansowego**, ma na celu uporządkowanie i harmonizację regulacji z obszaru zarządzania ICT w instytucjach finansowych. W sektorze finansowym regulacje te historycznie były zróżnicowane dla poszczególnych branż (bankowości, ubezpieczeń etc.), a także oparte na rozmaitych formatach regulacji — przepisach prawa, jak i wytycznych organów nadzoru. Rozporządzenie DORA tworzy nową i jednolitą strukturę tych regulacji dla sektora finansowego w całej Unii Europejskiej. Jej kluczowe postanowienia dotyczą m.in. ram zarządzania ryzykiem ICT, w szczególności przewidując dla niektórych podmiotów wymogi w zakresie regularnego testowania organizacji pod kątem odporności operacyjnej. Ponadto ujednolicony zostaje obszar zarządzania incydentami ICT, zwłaszcza raportowania ich do odpowiednich organów oraz współdzielenia się informacjami w zakresie cyberbezpieczeństwa.

[21] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011*.

Rozporządzenie DORA obejmuje instytucje finansowe takie jak banki, dostawcy płatności, zakłady ubezpieczeń, firmy inwestycyjne, dostawcy usług w zakresie kryptoaktywów, jak również zewnętrznych dostawców usług ICT.

W praktyce, ze względu na rozbudowany system kar administracyjnych, DORA znacznie podnosi ryzyko prawne niezgodności z regulacjami w zakresie ICT dla instytucji finansowych. Ponadto kluczowi dostawcy IT dla sektora (szczególnie tzw. Big Techy) zostaną objęci bezpośrednim nadzorem przez właściwe organy.

Ochrona konsumenta i usługi cyfrowe

Dyrektywy konsumenckie

Prawodawstwo Unii Europejskiej na przestrzeni ostatnich lat rozwinęło się w obszarze regulacji ochrony konsumenta, ze szczególnym naciskiem na sferę cyfrową[22]. **Dyrektywa Omnibus** (dyrektywa 2019/2161) wprowadziła wiele przepisów o istotnym znaczeniu dla handlu internetowego, zwłaszcza w zakresie zobowiązania przedsiębiorców do informowania o stosowanych przez nich cenach. Wymogi tej dyrektywy utrudniły nieuczciwe praktyki handlowe związane ze sztucznymi

[22] W szczególności: *Dyrektywa w sprawie umów o dostarczanie treści i usług cyfrowych (UE 2019/770)*, *Dyrektywa 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów*, *Dyrektywa 2019/2161 zmieniająca dyrektywę Rady 93/13/EWG i dyrektywy Parlamentu Europejskiego i Rady 98/6/WE, 2005/29/WE oraz 2011/83/UE w odniesieniu do lepszego egzekwowania i unowocześnienia unijnych przepisów dotyczących ochrony konsumenta* (dyrektywa Omnibus), *Dyrektywa 2020/1828 w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów*.

promocjami następującymi po uprzednim podniesieniu cen. Dyrektywa w sprawie umów dotyczących treści i usług cyfrowych oraz dyrektywa w sprawie niektórych aspektów umów sprzedaży towarów uregulowały obrót treściami i nowe zasady dotyczące sprzedaży dóbr zarówno cyfrowych, jak i materialnych, nakładając na przedsiębiorców obowiązki informacyjne. W krajowym porządku prawnym odpowiednie regulacje znajdują się zwłaszcza w **ustawie o prawach konsumenta** oraz **ustawie o świadczeniu usług drogą elektroniczną**. Regulacje te określają m.in. konieczność przygotowania właściwych regulaminów, a także prawa konsumenta w zakresie umów zawieranych na odległość. Mają fundamentalne znaczenie dla całej branży e-commerce.

Akt o usługach cyfrowych

Akt o usługach cyfrowych (*Digital Services Act*, DSA)[23] ma na celu poprawienie warunków funkcjonowania konsumentów i firm UE w internecie, w szczególności poprzez wprowadzenie nowych zasad dotyczących usług społeczeństwa informacyjnego, pośredników, platform i wyszukiwarek internetowych.

Kluczowe zagadnienia DSA w odniesieniu do platform internetowych obejmują m.in. obowiązek szybkiego usuwania nielegalnych treści z platform i doprecyzowanie zasad zwolnienia z odpowiedzialności oraz transparencji w zakresie algorytmów stosowanych przez **bardzo duże platformy internetowe** i **bardzo duże wyszukiwarki internetowe**[24].

[23] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE* (akt o usługach cyfrowych).

[24] Lista platform kwalifikowanych jako bardzo duże platformy internetowe dostępna jest na stronie Komisji Europejskiej, *https://ec.europa.eu/commis*
↪*sion/presscorner/detail/en/IP_23_2413*, dostęp 20.11.2023.

Te dwie ostatnie kategorie podmiotów są szczególnie traktowane, gdyż w DSA przewidziano dodatkowe wymagania oraz środki nadzorcze, jakie mogą być wobec nich stosowane — np. uprawnienie Komisji Europejskiej do wydawania poleceń w sytuacjach kryzysowych.

W ramach aktu o usługach cyfrowych sytuacja użytkownika internetu jest poprawiona m.in. przez ułatwienie zgłaszania nielegalnych treści, towarów lub usług na platformach internetowych oraz wprowadzenie obowiązkowej dostępności mechanizmów rozstrzygania sporów we własnym kraju. W związku z tym konsument w sporze z zagranicznym operatorem platformy nie jest skazany na poszukiwanie ochrony prawnej wyłącznie w odległej jurysdykcji. Dzięki obowiązkom w zakresie transparencji, zwłaszcza na platformach *marketplace*, użytkownikom łatwiej jest rozpoznawać faktycznego sprzedawcę produktów.

Jako element ochrony użytkownika wprowadzono również zakaz stosowania tzw. ***dark patterns***, czyli zwodniczych wzorców projektowych (zwodniczych interfejsów). Zwodnicze interfejsy to praktyki, które w istotny sposób zniekształcają lub ograniczają, celowo lub w praktyce, zdolność odbiorców usługi do dokonywania niezależnych i świadomych wyborów lub podejmowania takich decyzji. Jako ich przykłady można podać ukrywanie informacji lub wprowadzanie w błąd oraz ukrywanie lub utrudnianie możliwości rezygnacji z usługi.

Wprowadzono również ograniczenia w zakresie dozwolonej reklamy, zakazując m.in. **reklam ukierunkowanych** (tzw. targetowanych) opartych na danych wrażliwych (np.: orientacji seksualnej, religii, pochodzeniu etnicznym) i stosowania takich reklam wobec nieletnich.

Przyjęte przepisy stanowią istotną regulację dla przedsiębiorców działających w internecie, a ich praktyczna znajomość konieczna jest zwłaszcza w jednostkach odpowiadających za cyfrowe kanały sprzedaży i marketing.

Akt o rynkach cyfrowych

Akt o rynkach cyfrowych (*Digital Markets Act*, DMA)[25]**.** O ile regulacje szczególnie dedykowane dużym platformom internetowym pojawiają się w omawianym wyżej rozporządzeniu DSA w sposób wycinkowy, o tyle rozporządzenie DMA jest regulacją w zasadzie w całości poświęconą tzw. Big Techom. Interakcja pomiędzy tymi dwoma aktami prawnymi jest zamierzona. Uzupełniają się wzajemnie, tworząc kompleksową regulację usług cyfrowych w Unii Europejskiej.

Rynek usług cyfrowych jest obecnie zdominowany przez dużych graczy, często spoza Unii, dlatego na szczeblu unijnym podjęto decyzję o uregulowaniu zasad konkurencji w tym sektorze. Akt o rynkach cyfrowych ma zastosowanie do przedsiębiorstw, które zostaną uznane za **strażników dostępu** (ang. ***gatekeepers***). Stanowi o tym decyzja odpowiedniego organu podyktowana spełnieniem wymienionych w rozporządzeniu przesłanek, tj.

1) wywieranie znaczącego wpływu na rynek wewnętrzny;
2) świadczenie „podstawowej usługi platformowej", będącej ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych;
3) zajmowanie ugruntowanej i trwałej pozycji w zakresie prowadzonej przez siebie działalności lub możliwość przewidzenia, że zajmie się taką pozycję w niedalekiej przyszłości.

Poprzez **podstawowe usługi platformowe** z punktu 2 rozumie się m.in.: rynki internetowe, sklepy z aplikacjami, wyszukiwarki internetowe, internetowe serwisy społecznościowe, usługi przetwarzania w chmurze.

[25] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828* (akt o rynkach cyfrowych).

Przedsiębiorstwa zakwalifikowane jako strażnicy dostępu w drodze decyzji wydanej przez Komisję Europejską muszą w terminie sześciu miesięcy dostosować się do wymogów DMA[26].

Obowiązki strażników dostępu obejmują w szczególności zapewnienie dostępu do danych powstałych w wyniku korzystania z platformy strażnika dostępu, jak również do promocji swoich produktów i zawierania umów z klientami poza taką platformą. Reklamodawcy obecni na platformach strażników dostępu powinni zaś mieć dostęp do informacji na temat skuteczności realizowanych reklam.

Oprócz dodatkowych obowiązków strażnicy dostępu muszą też przestrzegać kilku zakazów, w ramach których zabroniono m.in.: traktowania własnych usług i produktów korzystniej niż analogicznych produktów podmiotów zewnętrznych, ponownego wykorzystywania prywatnych danych uzyskanych z jednej usługi na potrzeby innej usługi, wymuszania preinstalacji określonych aplikacji, uniemożliwiania twórcom aplikacji korzystania z niektórych rozwiązań (np. bramek płatniczych).

Regulacja ta w praktyce ma dość wąski zakres adresatów, którym w razie naruszeń grożą kary administracyjne. Świadomość wynikających z niej praw jest jednak bardzo istotna dla podmiotów rynku cyfrowego, zwłaszcza branży e-commerce. DMA w szczególności poprawia sytuację twórców aplikacji oraz firm prowadzących handel za pośrednictwem dużych platform internetowych.

[26] W chwili pisania tej książki KE wskazała sześć takich podmiotów. Lista jest dostępna na stronie KE, *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328*, dostęp 20.11.2023.

Elektroniczne podpisy i usługi zaufania

Ważnym elementem regulacji w obszarze IT są tzw. usługi identyfikacji elektronicznej i usługi zaufania. Obejmują one m.in. niezwykle spopularyzowane w ostatnich latach podpisy elektroniczne, które wciąż w praktyce nastręczają kłopotów — zwłaszcza co do rodzaju podpisu oraz wywoływanych skutków prawnych.

Obecne regulacje w tym zakresie obejmują **rozporządzenie EIDAS**[27], powiązaną z nim **ustawę o usługach zaufania oraz identyfikacji elektronicznej**, a także kluczowy dla praktyki w Polsce przepis **art. 78[1]** ***Kodeksu cywilnego***. Przyszłość tego typu rozwiązań będzie zaś kształtowana przez obecnie procedowane **rozporządzenie EIDAS 2**[28].

Rozporządzenie EIDAS wprowadziło do unijnego porządku regulację tzw. **usług zaufania**, czyli komercyjnych usług obejmujących tworzenie, weryfikację, walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego i certyfikatów powiązanych z tymi usługami. Zatem usługi w zakresie podpisów elektronicznych i podobnych mogą być świadczone jedynie przez certyfikowane podmioty, spełniające właściwe wymogi rozporządzenia — tzw. **dostawców zaufanych** (ang. ***trusted providers***). Ich lista wraz z opisem kwalifikowanych usług jest dostępna na odpowiedniej stronie internetowej[29].

---

[27] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*.

[28] Wniosek *Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej*, COM(2021) 281 final, 2021/0136(COD).

[29] *https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home*, dostęp 20.11.2023.

Warto zdawać sobie sprawę, że poza Unią Europejską nie wszędzie tak to funkcjonuje. Można znaleźć dokumenty, które zawierają różnego rodzaju podpisy elektroniczne, lecz te podpisy niekoniecznie będą uznawane w Unii. A nawet jeśli będą uznawane, to mogą nie wywoływać oczekiwanych przez nas skutków prawnych.

W rozporządzeniu EIDAS, jak wyżej wskazano, wymienia się kilka rodzajów usług zaufanych. Odzwierciedla to różnorodność rozwiązań, jakie przyjmowały się w poszczególnych krajach członkowskich, oraz ich skutków prawnych. W niektórych krajach jest popularna np. elektroniczna pieczęć, którą w Polsce spotyka się niezmiernie rzadko.

Na potrzeby polskiego obrotu kluczowa jest kategoria **kwalifikowanych podpisów elektronicznych**. Zgodnie bowiem z art. 78[1] *Kodeksu cywilnego* jedynie tego typu podpis jest równoznaczny z odręcznym podpisem na dokumencie:

> *§ 1 Do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym.*
>
> *§ 2 Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej.*

W konsekwencji wszystkie czynności, które ustawowo wymagają zachowania formy pisemnej pod rygorem nieważności, mogą być dokonane elektronicznie jedynie wtedy, gdy są opatrzone kwalifikowanym podpisem elektronicznym. Należy zatem bezwzględnie odróżniać tzw. zwykły podpis elektroniczny czy tzw. podpis zaufany od „kwalifikowanego" podpisu elektronicznego. Wedle polskiego ustawodawcy tylko ten drugi daje pewność, że osoba widniejąca na podpisie to faktycznie osoba, która go złożyła. Służą do tego odpowiednie zabezpieczenia. Tylko kwalifikowany podpis elektroniczny jest uważany za formę elektroniczną w rozumieniu *Kodeksu cywilnego*.

W praktyce należy więc weryfikować, czy podpis elektroniczny, jaki widzimy na dokumencie, spełnia odpowiednie wymogi EIDAS dla podpisu kwalifikowanego. Wykorzystuje się do tego programy komputerowe. Zalecana jest ostrożność w używaniu popularnych programów służących do otwierania plików PDF. Ich funkcjonalność niekiedy graficznie sugeruje poprawność podpisu (zielony znaczek), natomiast odnosi się to do każdego podpisu elektronicznego rozpoznawanego przez program. Sprawdzenie, czy jest to podpis kwalifikowany, wymaga weryfikacji właściwości podpisu. Alternatywnie — zastosowania specjalistycznego programu.

Pamiętajmy przy tym, że **podpisem elektronicznym nie jest jego graficzna reprezentacja**. Jeśli widzimy w dokumencie elektronicznym coś, co wygląda jak odręczny podpis, jest to jedynie element ozdobny. Podpis elektroniczny to ściśle określony zestaw danych, który może być wgrany do pliku stanowiącego podpisywany dokument albo być odrębnym plikiem. Decydujące jest tutaj powiązanie kryptograficzne pomiędzy danymi składającymi się na dokument a danymi składającymi się na podpis. Tym samym dokument, w którym jest widoczny „podpis", niekoniecznie jeszcze jest podpisany podpisem elektronicznym. Dlatego podpis weryfikujemy nie „na oko", tylko za pomocą odpowiedniego programu albo sprawdzając konkretne parametry dokumentu.

Dodatkowo, na podstawie art. 81 § 2 *Kodeksu cywilnego*, jeśli podpis kwalifikowany zawiera również tzw. kwalifikowany elektroniczny znacznik czasu (nie każdy podpis nim dysponuje), to dokument z takim podpisem nabiera waloru dokumentu z datą pewną. Niekiedy ma to znaczenie, np. przy umowach najmu (zob. np. art. 678 § 2 *Kodeksu cywilnego*).

W praktyce można spotkać się z wątpliwościami, czy wskazane reguły z art. 78^1 *Kodeksu cywilnego* (równoważność odręcznej formy pisemnej z elektroniczną) mają zastosowanie do popularnie zastrzeganej dla

zmian w umowie „formy pisemnej pod rygorem nieważności". O ile dominujący pogląd głosi, że tak — z czym należałoby się zgodzić — o tyle niektórzy autorzy prezentują bardziej formalistyczne podejście, które wymagałoby odpowiedniego zapisu w umowie. Wobec tego w praktyce bezpieczniej jest doprecyzować tę kwestię i zastrzegać w umowie, że formę elektroniczną strony uznają za równoważną formie pisemnej zastrzeżonej w umowie pod rygorem nieważności.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

PRAWO W IT

PRAKTYCZNIE I PO LUDZKU

Nieznajomość prawa szkodzi, a jego zrozumienie i umiejętność praktycznego stosowania są kluczowe dla skutecznego funkcjonowania w branży — również w obszarze IT.

Prawo w IT. Praktycznie i po ludzku to prawdziwe kompendium wiedzy nie tylko dla prawników, ale także specjalistów IT, menedżerów do spraw bezpieczeństwa informacji, wreszcie wszystkich tych, którym zależy na zrozumieniu i stosowaniu prawa w obszarze technologii informatycznych. Lektura niezbędna dla osób chcących się efektywnie poruszać w cyfrowej rzeczywistości i skutecznie chronić swoje interesy w świecie Internetu i nowych mediów.

Szymon Ciach, który specjalizuje się w umowach IT oraz regulacjach ICT w sektorze finansowym, używając żargonu właściwego dla branży IT, zagłębia się w najważniejsze aspekty regulacji prawnych związanych z cyberprzestrzenią, ochroną danych czy prawami autorskimi w świecie cyfrowym. Koncentruje się na wymiarze praktycznym omawianych zagadnień, co pozwala lepiej zrozumieć, jak działa prawo w odniesieniu do stanów faktycznych związanych z IT — nie tylko pokazuje zestaw istotnych przepisów, ale też wskazuje sposób myślenia, jaki można „zaimplementować", by radzić sobie ze stosowaniem prawa w tym obszarze.

W książce między innymi:

- **Świat IT okiem prawnika**
- **Umowy IT (rodzaje, najważniejsze zagadnienia)**
- **Technologie (chmura obliczeniowa, AI, DLT, blockchain, kryptoaktywa i więcej)**
- **Regulacje IT (przetwarzanie i ochrona danych, cyberbezpieczeństwo)**
- **Spory i transakcje M&A w IT**

Patronat:

iTWIZ.

Helion
onepress
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-8532-0
9 788328 385320

Cena: 89,00 zł