KOMISJA
EUROPEJSKA

Bruksela, dnia 24.7.2019 r.
COM(2019) 374 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Przepisy dotyczące ochrony danych jako czynnik sprzyjający zaufaniu w UE i poza nią – podsumowanie

Komunikat Komisji do Parlamentu Europejskiego i Rady:

Przepisy dotyczące ochrony danych jako czynnik sprzyjający zaufaniu w UE i poza nią – podsumowanie

I. Wprowadzenie

Ogólne rozporządzenie o ochronie danych[1] (zwane dalej „rozporządzeniem") stosuje się w całej Unii Europejskiej od ponad roku. Stanowi ono główny element spójnych i zmodernizowanych unijnych ram ochrony danych, które obejmują również dyrektywę o ochronie danych w sprawach karnych[2] oraz rozporządzenie dotyczące ochrony danych osobowych przez instytucje i organy UE[3]. Ramy te mają zostać uzupełnione rozporządzeniem w sprawie e-prywatności, które jest obecnie w trakcie procesu legislacyjnego.

Rygorystyczne przepisy dotyczące ochrony danych mają zasadnicze znaczenie dla zagwarantowania podstawowego prawa, jakim jest ochrona danych osobowych. Mają one kluczowe znaczenie dla demokratycznego społeczeństwa[4] oraz są ważnym elementem gospodarki w coraz większym stopniu opartej na danych. UE dąży do wykorzystania licznych możliwości, jakie stwarza transformacja cyfrowa w zakresie usług, zatrudnienia i innowacji, a jednocześnie stara się stawić czoła wyzwaniom, które wiążą się z tą transformacją. Kradzież tożsamości, wycieki danych wrażliwych, dyskryminacja osób fizycznych, wbudowana stronniczość, dzielenie się nielegalnymi treściami oraz opracowywanie naruszających prywatność narzędzi nadzoru to tylko kilka przykładów kwestii, które w coraz większym stopniu są przedmiotem debaty publicznej, i w przypadku których obywatele w sposób oczywisty oczekują, że ich dane będą chronione.

Ochrona danych stała prawdziwie globalnym zjawiskiem, ponieważ ludzie na całym świecie coraz bardziej cenią ochronę i bezpieczeństwo swoich danych. Wiele krajów przyjęło lub jest

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1): https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex:32016L0680. Państwa członkowskie miały dokonać transpozycji tej dyrektywy do dnia 6 maja 2018 r. Sprawozdania dotyczące unii bezpieczeństwa zawierają informacje na temat stanu transpozycji wymienionej dyrektywy.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE, Dz.U. L 295 z 21.11.2018, s. 39-98: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32018R1725. Jego przepisy zaczęto stosować od dnia 11 grudnia 2018 r.

[4] W przełomowym wyroku z dnia 24 sierpnia 2017 r. Sąd Najwyższy Indii uznał, że prywatność jest prawem podstawowym, „jednym z podstawowych aspektów godności ludzkiej".

w trakcie przyjmowania kompleksowych przepisów o ochronie danych w oparciu o zasady podobne do zasad zawartych w rozporządzeniu, co prowadzi do zbieżności przepisów o ochronie danych na całym świecie. Stwarza to nowe możliwości ułatwiania przepływu danych między operatorami komercyjnymi lub organami publicznymi, przy jednoczesnym zwiększeniu poziomu ochrony danych osobowych w UE i na całym świecie.

Ochrona danych jest traktowana poważniej niż kiedykolwiek wcześniej i ma daleko idący wpływ na wiele zainteresowanych stron i sektorów. Komisja pragnie sprawić, by UE skutecznie wdrażała nowy system ochrony danych, oraz zdecydowanie wspiera osiągnięcie pełnej zdolności operacyjnej przez wszystkie jego elementy. W niniejszym komunikacie Komisja podsumowuje osiągnięte dotychczas wyniki w odniesieniu do spójnego wdrażania przepisów o ochronie danych w całej UE, funkcjonowania nowego systemu zarządzania, wpływu na obywateli i przedsiębiorstwa oraz wysiłków UE na rzecz propagowania konwergencji w zakresie systemów ochrony danych. Niniejszy komunikat został opracowany w następstwie komunikatu Komisji w sprawie stosowania rozporządzenia ze stycznia 2018 r.[5] i opiera się na wynikach prac wielostronnej grupy zainteresowanych stron[6], w szczególności na jej wkładzie w roczne podsumowanie sytuacji, a także na dyskusjach przeprowadzonych podczas spotkania podsumowującego zorganizowanego przez Komisję w dniu 13 czerwca 2019 r.[7]. Niniejszy komunikat stanowi również wkład w przegląd, który Komisja planuje przeprowadzić do maja 2020 r. [8]

Unijne ramy prawne w zakresie ochrony danych stanowią fundament europejskiego podejścia do innowacji ukierunkowanego na człowieka. Stają się częścią podstawy regulacyjnej dla coraz szerszego zakresu polityk, w tym polityk w dziedzinie zdrowia i badań naukowych, sztucznej inteligencji, transportu, energii, konkurencji oraz egzekwowania prawa. Komisja konsekwentnie podkreślała znaczenie właściwego wdrażania i egzekwowania nowych przepisów dotyczących ochrony danych, co podkreśliła w komunikacie w sprawie stosowania rozporządzenia ze stycznia 2018 r. oraz w wytycznych z września 2018 r. dotyczących wykorzystywania danych osobowych w kontekście wyborczym[9]. W momencie opracowywania niniejszego komunikatu poczyniono znaczne postępy w realizacji tego celu, choć z pewnością potrzebne są dalsze prace, aby rozporządzenie funkcjonowało w pełni.

---

5 Komunikat Komisji do Parlamentu Europejskiego i Rady „Wzmocniona ochrona, nowe możliwości – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych od dnia 25 maja 2018 r.”, COM(2018) 43 final: https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 Ustanowiona przez Komisję wielostronna grupa zainteresowanych stron ds. rozporządzenia obejmuje przedstawicieli społeczeństwa obywatelskiego, biznesu, środowisk akademickich i osób zawodowo zajmujących się przedmiotowymi zagadnieniami: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

7 http://europa.eu/rapid/press-release_IP-19-2956_pl.htm.

8 Art. 97 rozporządzenia.

9 „Wytyczne Komisji dotyczące stosowania unijnych przepisów o ochronie danych osobowych w kontekście wyborczym”, COM (2018) 638 final; https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1567687466030&uri=CELEX:52018DC0638.

II. Jeden kontynent – jedno prawo: ramy ochrony danych obowiązują w państwach członkowskich

Jednym z głównych celów rozporządzenia było usunięcie rozdrobnionego systemu obejmującego 28 różnych zbiorów przepisów krajowych istniejącego na mocy poprzedniej dyrektywy o ochronie danych[10] oraz zapewnienie pewności prawnej dla osób fizycznych i przedsiębiorstw w całej UE. Cel ten został w dużej mierze osiągnięty.

Harmonizacja ram prawnych

Chociaż rozporządzenie jest bezpośrednio stosowane w państwach członkowskich, zobowiązuje je do podjęcia szeregu kroków prawnych na szczeblu krajowym, w szczególności do ustanowienia krajowych organów ochrony danych i przyznania im uprawnień[11], ustanowienia przepisów dotyczących konkretnych kwestii, takich jak pogodzenie ochrony danych osobowych z wolnością wypowiedzi i informacji, oraz do zmiany lub uchylenia prawodawstwa sektorowego, które zawiera aspekty ochrony danych. W chwili opracowywania niniejszego komunikatu wszystkie państwa członkowskie z wyjątkiem trzech[12] zaktualizowały krajowe przepisy o ochronie danych. Na szczeblu krajowym wciąż trwają prace nad dostosowaniem przepisów sektorowych. Po włączeniu rozporządzenia do Porozumienia o Europejskim Obszarze Gospodarczym jego stosowanie rozszerzono na Norwegię, Islandię i Liechtenstein, które również przyjęły krajowe przepisy o ochronie danych.

Zainteresowane strony domagają się jednak jeszcze większego stopnia harmonizacji w niektórych dziedzinach[13]. Rozporządzenie daje bowiem państwom członkowskim możliwość dalszego sprecyzowania jego stosowania w niektórych obszarach, takich jak minimalny wiek wyrażenia zgody przez dzieci na usługi online[14] lub przetwarzanie danych osobowych w takich dziedzinach jak medycyna i zdrowie publiczne. W takim przypadku działania państw członkowskich podlegają następującym dwóm wymogom:

i) wszelkie krajowe przepisy doprecyzowujące muszą spełniać wymogi Karty praw podstawowych[15] (i nie wykraczać poza ograniczenia określone w rozporządzeniu, które opiera się na Karcie);
ii) nie mogą rzutować na swobodny przepływ danych osobowych w UE[16].

---

[10] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:31995L0046.

[11] Takich jak uprawnienie do nakładania administracyjnych kar pieniężnych.

[12] W dniu 23 lipca 2019 r. Grecja, Portugalia i Słowenia są nadal w trakcie przyjmowania swoich przepisów krajowych.

[13] Zob. sprawozdanie wielostronnej grupy zainteresowanych stron ds. rozporządzenia z dnia 13 czerwca 2019 r.: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

[14] 13 lat w przypadku Belgii, Danii, Estonii, Finlandii, Łotwy, Malty, Szwecji i Zjednoczonego Królestwa; 14 lat w przypadku Austrii, Bułgarii, Cypru, Hiszpanii, Włoch i Litwy; 15 lat w przypadku Czech i Francji; 16 lat w przypadku Niemiec, Węgier, Chorwacji, Irlandii, Luksemburga, Niderlandów, Polski, Rumunii i Słowacji.

[15] Art. 8.

W niektórych przypadkach państwa członkowskie wprowadziły wymogi krajowe wykraczające poza rozporządzenie, w szczególności w drodze wielu przepisów sektorowych, co prowadzi do fragmentacji i powoduje powstawanie niepotrzebnych obciążeń. Jednym z przykładów dodatkowego wymogu wprowadzonego przez państwa członkowskie oprócz rozporządzenia jest wprowadzony przez ustawodawstwo niemieckie obowiązek wyznaczenia inspektora ochrony danych w przedsiębiorstwach zatrudniających co najmniej 20 pracowników zaangażowanych w automatyczne przetwarzanie danych osobowych.

Dalsze starania na rzecz większej harmonizacji

Komisja angażuje się w dwustronny dialog z organami krajowymi, w ramach którego zwraca szczególną uwagę na środki krajowe dotyczące:

- faktycznej niezależności organów ochrony danych, w tym za pomocą odpowiednich zasobów finansowych, ludzkich i technicznych;
- sposobu, w jaki przepisy krajowe ograniczają prawa osób, których dane dotyczą;
- faktu, że przepisy krajowe nie powinny wprowadzać wymogów wykraczających poza zakres rozporządzenia, jeżeli nie istnieje możliwość wprowadzania precyzyjniejszych przepisów, takich jak dodatkowe warunki przetwarzania;
- wywiązywania się z obowiązku pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji, przy uwzględnieniu faktu, że obowiązek ten nie powinien być nadużywany do wywierania efektu mrożącego na pracę dziennikarską.

Praca organów ochrony danych, współpracujących w ramach Europejskiej Rady Ochrony Danych (zwanej dalej „radą"), stanowi kluczowy czynnik przyczyniający się do spójnego stosowania nowych przepisów: działania w zakresie egzekwowania prawa mające wpływ na kilka państw członkowskich przechodzą przez mechanizm współpracy i spójności[17] w ramach rady, a wytyczne przyjęte przez radę przyczyniają się do jednolitego rozumienia rozporządzenia. Niemniej jednak zainteresowane strony oczekują od organów ochrony danych dalszych działań w tym kierunku.

Praca sądów krajowych i Trybunału Sprawiedliwości Unii Europejskiej pomaga również w tworzeniu spójnej wykładni przepisów w dziedzinie ochrony danych. Sądy krajowe wydały ostatnio wyroki w sprawie unieważnienia przepisów prawa krajowego, które odbiegają od przepisów rozporządzenia[18].

---

[16] Zgodnie z art. 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej.

[17] Art. 60 rozporządzenia przewiduje współpracę między organami ochrony danych w zakresie stosowania jednej wykładni rozporządzenia w konkretnych przypadkach. Art. 64 stanowi, że w niektórych przypadkach rada wydaje opinie w celu zapewnienia spójnego stosowania rozporządzenia. Ponadto rada ma prawo do przyjmowania wiążących decyzji skierowanych do organów ochrony danych w przypadku braku zgody między nimi.

[18] Tak było w przypadku Niemiec i Hiszpanii.

III. Wszystkie elementy nowego systemu zarządzania układają się w logiczną całość.

W rozporządzeniu utworzono nową strukturę zarządzania, której kluczowym elementem są niezależne krajowe organy ochrony danych, jako podmioty odpowiedzialne za egzekwowanie przepisów rozporządzenia oraz pierwsze punkty kontaktowe dla zainteresowanych stron. Chociaż w ostatnim roku większość organów ochrony danych korzystała ze zwiększonych środków, nadal istnieją ogromne różnice między państwami członkowskimi[19].

Organy ochrony danych korzystają ze swoich nowych uprawnień

Rozporządzenie wyposaża organy ochrony danych w szersze uprawnienia wykonawcze. Wbrew obawom wyrażonym przez niektóre zainteresowane strony przed majem 2018 r. krajowe organy ochrony danych przyjęły zrównoważone podejście do uprawnień wykonawczych. Koncentrowały się one na dialogu, a nie na sankcjach, w szczególności w odniesieniu do najmniejszych podmiotów gospodarczych, dla których przetwarzanie danych osobowych nie jest podstawową działalnością. Jednocześnie organy te nie cofały się w razie potrzeby przed faktycznym wykorzystywaniem swoich nowych uprawnień, w tym poprzez wszczynanie postępowań dotyczących mediów społecznościowych[20] oraz nakładanie administracyjnych kar pieniężnych w wysokości od kilku tysięcy euro do kilku milionów euro, w zależności od wagi naruszenia przepisów o ochronie danych.

Przykłady kar pieniężnych nałożonych przez organy ochrony danych[21]:

- 5 000 EUR kary dla punktu zakładów sportowych w Austrii za niezgodny z prawem nadzór wideo;
- 220 000 EUR kary dla przedsiębiorstwa pośredniczącego w obrocie danymi w Polsce za brak poinformowania osób fizycznych o tym, że ich dane są przetwarzane;
- 250 000 EUR kary dla hiszpańskiej ligi piłki nożnej LaLiga, za brak przejrzystości jej aplikacji na smartfony;
- 50 mln EUR kary dla Google we Francji za nieodpowiednie warunki uzyskania zgody od użytkowników.

W trakcie prowadzenia postępowań ważne jest, aby organy ochrony danych gromadziły odpowiednie dowody, przestrzegały wszystkich etapów procedury zgodnie z ustawodawstwem krajowym oraz zapewniały poszanowanie procedur w często skomplikowanych sprawach. Wymaga to czasu oraz znacznego nakładu pracy, co wyjaśnia, dlaczego większość postępowań wszczętych po rozpoczęciu stosowania rozporządzenia jest nadal w toku.

---

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

20 Na przykład irlandzka Komisja ds. Ochrony Danych wszczęła 15 formalnych postępowań wyjaśniających w odniesieniu do przestrzegania przepisów rozporządzenia przez wielonarodowe przedsiębiorstwa technologiczne. Zob. s. 49 sprawozdania rocznego irlandzkiej Komisji ds. Ochrony Danych z 2018 r.: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Niektóre z decyzji o nałożeniu kar pieniężnych są nadal przedmiotem kontroli sądowej.

Skuteczność rozporządzenia nie powinna jednak być mierzona liczbą nałożonych kar pieniężnych, lecz zmianami w kulturze i zachowaniu wszystkich zaangażowanych podmiotów. W tym kontekście organy ochrony danych dysponują innymi narzędziami, takimi jak tymczasowe lub ostateczne ograniczenie przetwarzania, w tym zakaz lub nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim[22].

Niektóre organy ochrony danych stworzyły nowe narzędzia, takie jak infolinie i podręczniki dla przedsiębiorstw, podczas gdy inne opracowały nowatorskie podejścia, m.in. tzw. „piaskownice regulacyjne"[23], aby pomóc przedsiębiorstwom w ich działaniach na rzecz przestrzegania przepisów. Jednak niektóre zainteresowane strony, w szczególności małe i średnie przedsiębiorstwa w niektórych państwach członkowskich[24], nadal uważają, że nie otrzymały wystarczającego wsparcia i informacji. Aby zaradzić tej sytuacji, Komisja udziela dotacji organom ochrony danych w celu dotarcia do zainteresowanych stron, w szczególności do osób fizycznych oraz małych i średnich przedsiębiorstw[25].

Europejska Rada Ochrony Danych osiągnęła zdolność operacyjną

Organy ochrony danych zintensyfikowały swoje prace w ramach Europejskiej Rady Ochrony Danych[26]. Ta intensywna praca pozwoliła radzie na przyjęcie około 20 wytycznych w sprawie kluczowych aspektów rozporządzenia[27]. Przyszłe obszary pracy rady zostały przedstawione w 2-letnim programie[28] zgodnie z wymogami rozporządzenia.

W przypadku spraw transgranicznych każdy organ ochrony danych nie jest już wyłącznie organem krajowym, ale częścią prawdziwie ogólnounijnego procesu na wszystkich etapach, od postępowania wyjaśniającego aż do decyzji. Taka bliska współpraca stała się codzienną praktyką: do końca czerwca 2019 r. za pośrednictwem mechanizmu współpracy rozpatrzono 516 spraw transgranicznych.

Komisja aktywnie przyczynia się do prac rady[29] mających na celu propagowanie litery i ducha rozporządzenia oraz przypomina o ogólnych zasadach prawa UE[30].

---

22 Art. 58 ust. 2 lit. f) i j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/

24 Zob. sprawozdanie wielostronnej grupy zainteresowanych stron ds. rozporządzenia: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670

25 W 2018 r. dziewięciu organom ochrony danych przydzielono kwotę 2 mln EUR na działania w latach 2018-2019: w Belgii, Bułgarii, Danii, na Węgrzech, Litwie, Łotwie, w Niderlandach, Słowenii i Islandii: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
W 2019 r. ma zostać przyznana kwota 1 mln EUR: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Rada posiada osobowość prawną, a w jej skład wchodzą dyrektorzy krajowych organów nadzorczych ds. ochrony danych oraz Europejski Inspektor Ochrony Danych.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_pl

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_pl

29 W charakterze uczestnika bez prawa głosu.

30 Komisja pomogła również w sprawnym ustanowieniu rady i wspiera jej funkcjonowanie poprzez udostępnienie swojego systemu komunikacji.

Dążenie do stworzenia unijnej kultury ochrony danych

Nowy system zarządzania musi jeszcze w pełni rozwinąć swój potencjał. Ważne jest, aby rada w dalszym ciągu usprawniała swój proces podejmowania decyzji i stworzyła wspólną unijną kulturę ochrony danych wśród swoich członków. Możliwość połączenia wysiłków[31] organów ochrony danych w kwestiach dotyczących więcej niż jednego państwa członkowskiego, na przykład w celu przeprowadzenia wspólnych postępowań i działań egzekucyjnych, mogą przyczynić się do osiągnięcia takiego celu, jednocześnie redukując ograniczenia związane z zasobami.

Wiele zainteresowanych stron opowiada się za jeszcze ściślejszą współpracą i jednolitym podejściem ze strony krajowych organów ochrony danych[32]. Wnoszą również o większą spójność porad udzielanych przez organy ochrony danych[33] oraz o pełną zgodność wytycznych krajowych z wytycznymi rady. Niektóre ze stron oczekują również dalszego doprecyzowania kluczowych pojęć rozporządzenia, takich jak podejście oparte na analizie ryzyka, ze szczególnym uwzględnieniem obaw zwłaszcza małych i średnich przedsiębiorstw.

W tym kontekście zasadnicze znaczenie ma umożliwienie zainteresowanym stronom większego udziału w pracach rady. Dlatego też Komisja z zadowoleniem przyjmuje organizowane przez radę systematyczne publiczne konsultacje w sprawie wytycznych. Praktyka ta oraz organizacja warsztatów dla zainteresowanych stron dotyczących konkretnych tematów na wczesnym etapie refleksji, powinny być kontynuowane i rozwijane w celu zapewnienia przejrzystości, inkluzywności i adekwatności prac rady.

IV. Osoby fizyczne korzystają z przysługujących im praw, ale należy kontynuować zwiększanie świadomości w tej dziedzinie

Innym kluczowym celem rozporządzenia było wzmocnienie praw osób fizycznych. Rozporządzenie uznawane jest powszechnie przez stowarzyszenia praw obywatelskich i organizacje konsumenckie za istotny wkład w sprawiedliwe społeczeństwo cyfrowe oparte na wzajemnym zaufaniu.

Większa świadomość na temat praw do ochrony danych

Osoby fizyczne w UE są coraz bardziej świadome przepisów dotyczących ochrony danych i własnych praw: 67 % respondentów, którzy wzięli udział w badaniu Eurobarometru z maja 2019 r.[34], wie o rozporządzeniu, a 57 % ma świadomość, że istnieje krajowy organ ochrony danych, do którego mogą zwracać się o informacje lub składać skargi. 73 % z nich słyszało o

---

31 Art. 62 rozporządzenia.

32 Zob. sprawozdanie wielostronnej grupy zainteresowanych stron ds. rozporządzenia: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Przedsiębiorstwa uważają na przykład, że można było lepiej zharmonizować krajowe wykazy rodzajów operacji przetwarzania, które wymagają oceny skutków dla ochrony danych, o której mowa w art. 35 rozporządzenia.

33 W tym pomiędzy poszczególnymi organami w krajach związkowych.

34 http://europa.eu/rapid/press-release_IP-19-2956_pl.htm

co najmniej jednym z praw przyznanych na mocy rozporządzenia. Jednak znaczna liczba osób w UE nadal nie podejmuje aktywnych działań w celu ochrony swoich danych osobowych podczas korzystania z internetu. Na przykład 44 % osób nie zmieniło swoich domyślnych ustawień prywatności w sieciach społecznościowych.

Obywatele coraz częściej korzystają ze swoich praw

Dzięki większej świadomości swoich praw osoby fizyczne mogły z nich korzystać efektywniej poprzez zadawanie pytań oraz częstsze zwracanie się do organów ochrony danych z prośbą o informacje lub w celu złożenia skargi[35]. Przedsiębiorstwa zgłaszają również, że liczba wniosków o dostęp do danych osobowych wzrosła w kilku sektorach, między innymi w bankowości i telekomunikacji. Osoby fizyczne również częściej wycofywały swoją zgodę i korzystały z prawa sprzeciwu wobec przekazów handlowych[36].

Niektóre podmioty zgłaszały jednak brak zrozumienia ze strony osób fizycznych przepisów o ochronie danych, m.in. przekonanie, że osoby fizyczne powinny wyrazić zgodę na wszelkie przetwarzanie danych lub że prawo do usunięcia danych ma charakter bezwzględny (podczas gdy dane osobowe muszą czasami być przechowywane przez podmioty gospodarcze ze względu na zobowiązania prawne)[37]. Organizacje społeczeństwa obywatelskiego skarżą się natomiast na znaczne opóźnienia w udzielaniu odpowiedzi przez niektóre przedsiębiorstwa i organy ochrony danych.

Co istotne, kilka powództw przedstawicielskich zostało wszczętych przez organizacje pozarządowe upoważnione przez osoby fizyczne, z wykorzystaniem nowej możliwości przewidzianej w rozporządzeniu[38]. Korzystanie z powództw przedstawicielskich byłoby łatwiejsze, gdyby więcej państw członkowskich dopuszczało możliwość przewidzianą w rozporządzeniu, zgodnie z którą organizacje pozarządowe mogą wszczynać powództwa bez mandatu[39].

Potrzeba kontynuowania działań na rzecz zwiększania świadomości

W związku z tym należy kontynuować dialog i działania informacyjne skierowane do ogółu społeczeństwa na szczeblu krajowym i unijnym. W tym celu w lipcu 2019 r. Komisja rozpoczęła nową kampanię internetową[40], aby zachęcić osoby fizyczne do zapoznawania się z oświadczeniami o ochronie prywatności oraz do optymalizacji swoich ustawień prywatności.

---

35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf

36 Zob. sprawozdanie wielostronnej grupy zainteresowanych stron ds. ogólnego rozporządzenia o ochronie danych.

37 Zob. sprawozdanie wielostronnej grupy zainteresowanych stron ds. ogólnego rozporządzenia o ochronie danych.

38 Art. 80 ust. 1 rozporządzenia.

39 Art. 80 ust. 2 rozporządzenia.

40 Kampania ta jest kontynuacją wcześniejszej kampanii mającej na celu rozpowszechnianie materiałów informacyjnych dla osób fizycznych i przedsiębiorstw, które są dostępne na stronie internetowej: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pl.

V. Przedsiębiorstwa dostosowują swoje praktyki

Rozporządzenie ma na celu wspieranie przedsiębiorstw w gospodarce cyfrowej przez proponowanie rozwiązań dostosowanych do przyszłych wyzwań. Zasadniczo przedsiębiorstwa z zadowoleniem przyjmują zasadę odpowiedzialności zawartą w rozporządzeniu, która odchodzi od poprzedniego i uciążliwego podejścia *ex ante* (zniesienie wymogów w zakresie powiadamiania, skalowalność obowiązków i elastyczność zasady uwzględniania ochrony danych już w fazie projektowania oraz domyślnej ochrony danych, która umożliwia konkurencję w oparciu o rozwiązania przyjazne dla prywatności). Jednocześnie niektóre z nich domagają się większej pewności prawnej oraz dodatkowych lub jaśniejszych wytycznych ze strony organów ochrony danych[41].

Należyte zarządzanie danymi

Chociaż przedsiębiorstwa informują o wielu wyzwaniach związanych z dostosowaniem do nowych przepisów[42], wiele z nich podkreśla, że jest to również okazja do zwrócenia uwagi zarządów spółek na kwestię ochrony danych, uporządkowania posiadanych przez nie danych, poprawy bezpieczeństwa, lepszego przygotowania na incydenty, zmniejszenia narażenia na niepotrzebne ryzyko oraz budowania stosunków z klientami i partnerami handlowymi opartych w większym stopniu na zaufaniu. Jeśli chodzi o przejrzystość, organizacje biznesowe i organizacje społeczeństwa obywatelskiego zaznaczyły, że niełatwo jest osiągnąć równowagę między przekazaniem osobom fizycznym wszystkich wymaganych informacji wynikających z rozporządzenia, a jednocześnie stosowaniem jasnego i prostego języka i formy, zrozumiałych dla wszystkich. Podmioty gospodarcze opracowują innowacyjne rozwiązania w tym kierunku.

Ogólnie rzecz biorąc, przedsiębiorstwa wskazały, że są w stanie wdrażać nowe prawa osób, których dane dotyczą, chociaż czasami wyzwaniem było dotrzymanie terminów w związku z dużą liczbą wniosków i ich szerszym zakresem[43] lub sprawdzenie tożsamości osoby składającej wniosek.

Wpływ na innowacje

Rozporządzenie nie tylko umożliwia rozwój nowych technologii, lecz także sprzyja temu rozwojowi, przy jednoczesnym poszanowaniu podstawowego prawa do ochrony danych osobowych. Dotyczy to takich obszarów jak sztuczna inteligencja.

Przedsiębiorstwa zaczęły rozwijać ofertę nowych usług bardziej przyjaznych dla ochrony prywatności. Przykładowo wyszukiwarki, które nie śledzą użytkowników lub nie stosują reklamy behawioralnej, zdobywają coraz większy udział w rynku w niektórych państwach

---

41 Zob. sprawozdanie wielostronnej grupy zainteresowanych stron ds. rozporządzenia.

42 Aktualizacja systemu informatycznego jest często wymieniana jako jedno z głównych wyzwań, w szczególności w odniesieniu do wdrażania zasad uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych, prawa do usunięcia danych w kopii zapasowej itp.

43 Przedsiębiorstwa wnioskują również o wytyczne rady w sprawie nieuzasadnionych i nadmiernych wniosków.

członkowskich. Inne przedsiębiorstwa opracowują usługi, które opierają się na nowych prawach przyznanych osobom fizycznym, takich jak możliwość przenoszenia swoich danych osobowych. Coraz więcej przedsiębiorstw promuje poszanowanie danych osobowych jako konkurencyjny element wyróżniający oraz swój atut. Zmiany te nie ograniczają się do UE, lecz dotyczą również bardzo innowacyjnych gospodarek zagranicznych[44].

Szczególna sytuacja mikroprzedsiębiorstw i małych przedsiębiorstw „niskiego ryzyka"

Pomimo iż sytuacja różni się w poszczególnych państwach członkowskich, to mikroprzedsiębiorstwa i małe przedsiębiorstwa[45], których główną działalnością nie jest przetwarzanie danych osobowych, zadają najwięcej pytań odnośnie do stosowania rozporządzenia. Chociaż wydaje się, że liczba pytań częściowo wynika z niewystarczającej wiedzy na temat przepisów o ochronie danych, ich obawy są czasami potęgowane przez kampanie przedsiębiorstw świadczących płatne usługi doradcze, przez rozpowszechnianie błędnych informacji, na przykład o konieczności systematycznego uzyskiwania zgody osób fizycznych[46] oraz przez dodatkowe wymogi nakładane na szczeblu krajowym.

W tym kontekście mikroprzedsiębiorstwa i małe przedsiębiorstwa wzywają do opracowania wytycznych dostosowanych do ich konkretnej sytuacji oraz zawierających bardzo praktyczne informacje. Niektóre organy ochrony danych już tego dokonały na szczeblu krajowym[47]. W celu uzupełnienia inicjatyw krajowych Komisja wydała materiały informacyjne mające pomóc takim przedsiębiorstwom w dostosowaniu się do nowych przepisów poprzez podjęcie szeregu praktycznych kroków[48].

Wykorzystywanie zestawu narzędzi przewidzianych w rozporządzeniu

W rozporządzeniu przewidziano narzędzia do wykazania zgodności, takie jak standardowe klauzule umowne, kodeksy postępowania oraz nowo wprowadzone mechanizmy certyfikacji.

Standardowe klauzule umowne to klauzule wzorcowe, które można zawrzeć w umowie na zasadzie dobrowolności, na przykład między administratorem danych a podmiotem przetwarzającym dane, i które określają obowiązki stron umowy wynikające z rozporządzenia. Rozporządzenie rozszerza możliwości stosowania standardowych klauzul umownych zarówno w przypadku międzynarodowego przekazywania danych[49], jak

---

[44] Na przykład, zgodnie ze sprawozdaniem opublikowanym przez izraelskie stowarzyszenie przemysłu cyberbezpieczeństwa, w 2018 r. podsektor „ochrona danych i prywatność" stanowił najszybciej rosnący podsektor cyberbezpieczeństwa, co jest częściowo skutkiem wejścia w życie ogólnego rozporządzenia o ochronie danych.

[45] Zgodnie z definicją MŚP dostępną na stronie internetowej: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_pl.

[46] W rzeczywistości rozporządzenie nie opiera się wyłącznie na zgodzie, lecz przewiduje szereg podstaw prawnych dla przetwarzania danych osobowych.

[47] Przykładowo przewodnik opracowany przez francuski organ ochrony danych: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

[48] https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-pl-n.pdf.

[49] Zob. art. 28 rozporządzenia. Standardowe klauzule umowne przyjęte przez Komisję mają zastosowanie w całej UE. Natomiast klauzule przyjęte na podstawie art. 28 ust. 8 przez organ ochrony danych są wiążące jedynie dla organu, który je przyjął, i mogą być zatem stosowane jako standardowe klauzule umowne

i wewnątrz UE. W dziedzinie międzynarodowego przekazywania danych szerokie stosowanie tych klauzul wskazuje[50], że są one bardzo pomocne dla przedsiębiorstw przy zapewnianiu zgodności z przepisami, a w szczególności dla przedsiębiorstw, które nie posiadają zasobów do negocjowania indywidualnych umów z każdym ze swoich kontrahentów przetwarzających dane.

Podmioty w wielu sektorach uważają również przyjęcie standardowych klauzul umownych za użyteczny sposób wspierania harmonizacji, w szczególności gdy zostały one przyjęte przez Komisję. Komisja będzie współpracowała z zainteresowanymi stronami, aby wykorzystać możliwości przewidziane w rozporządzeniu i zaktualizować istniejące klauzule.

Przestrzeganie kodeksów postępowania jest kolejnym narzędziem operacyjnym i praktycznym, którym dysponują przedsiębiorstwa w celu łatwiejszego wykazania zgodności z rozporządzeniem[51]. Kodeksy te powinny być opracowywane przez stowarzyszenia branżowe lub podmioty reprezentujące określone kategorie administratorów i podmiotów przetwarzających oraz powinny opisywać, w jaki sposób można wdrożyć przepisy o ochronie danych w danym sektorze. Poprzez dostosowanie obowiązków do istniejącego ryzyka[52] kodeksy te mogą również okazać się bardzo przydatnym i opłacalnym sposobem wypełnienia zobowiązań przez małe i średnie przedsiębiorstwa.

Ponadto certyfikacja może być również przydatnym instrumentem wykazania zgodności z konkretnymi wymogami rozporządzenia. Może ona zwiększyć pewność prawa dla przedsiębiorstw i promować stosowanie rozporządzenia na całym świecie. Niedawno przyjęte przez Europejską Radę Ochrony Danych wytyczne[53] w zakresie certyfikacji i akredytacji umożliwią rozwój systemów certyfikacji w UE. Komisja będzie monitorować te zmiany oraz, w stosownych przypadkach, wykorzysta uprawnienia przewidziane w rozporządzeniu w celu określenia wymogów w zakresie certyfikacji. Komisja może również zwrócić się do unijnych organów normalizacyjnych z wnioskiem o normalizację elementów istotnych dla rozporządzenia.

VI. Pozytywna konwergencja postępuje na szczeblu międzynarodowym

Zapotrzebowanie na ochronę danych osobowych nie ogranicza się wyłącznie do UE. Jak pokazuje niedawny globalny sondaż na temat bezpieczeństwa w internecie, na całym świecie

---

w odniesieniu do operacji przetwarzania, które wchodzą w zakres jurysdykcji tego organu, zgodnie z art. 55 i 56.

50 Są one w rzeczywistości głównym narzędziem, na którym przedsiębiorstwa opierają się podczas eksportu danych.

51 Europejska Rada Ochrony Danych przyjęła w dniu 4 czerwca 2019 r. wytyczne w sprawie kodeksów postępowania. Wyjaśniają one procedury i zasady dotyczące przedstawiania, zatwierdzania i publikowania kodeksów, zarówno na szczeblu krajowym, jak i na szczeblu UE.

52 Motyw 98 rozporządzenia.

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_pl; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_pl

pogłębia się deficyt zaufania, co sprawia, że ludzie zmieniają swoje zachowania online[54]. Coraz większa liczba przedsiębiorstw stara się rozwiązać te problemy poprzez rozszerzenie z własnej inicjatywy praw wynikających z rozporządzenia na swoich klientów spoza UE.

Ponadto, jako że kraje na całym świecie w coraz większym stopniu mierzą się z podobnymi wyzwaniami, tworzą nowe przepisy o ochronie danych lub modernizują istniejące. Przepisy te często mają szereg wspólnych cech z unijnym systemem ochrony danych, takich jak nadrzędne przepisy (a nie przepisy sektorowe), możliwe do wyegzekwowania prawa indywidualne oraz niezależny organ nadzorczy. Tendencja ta ma charakter globalny, od Korei Południowej po Brazylię, od Chile po Tajlandię i od Indii po Indonezję. Coraz większa liczba państw, które przystąpiły do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych Rady Europy (ETS nr 108)[55] – ostatnio zaktualizowanej[56] przy znaczącym wkładzie ze strony Komisji – jest kolejną wyraźną oznaką tendencji pozytywnej konwergencji.

Promowanie bezpiecznych i swobodnych przepływów danych poprzez decyzje stwierdzające odpowiedni stopień ochrony danych osobowych i poza nimi

Ta postępująca konwergencja stwarza nowe możliwości ułatwiania przepływów danych, a tym samym wymiany handlowej, a także współpracy między organami publicznymi, przy jednoczesnym zwiększeniu poziomu ochrony danych osób fizycznych w UE w przypadku ich przekazywania za granicę.

W ramach realizacji strategii przedstawionej w komunikacie z 2017 r. w sprawie wymiany i ochrony danych osobowych w zglobalizowanym świecie[57] Komisja zwiększyła swoje zaangażowanie we współpracę z państwami trzecimi i innymi partnerami międzynarodowymi, wykorzystując i rozwijając elementy konwergencji między systemami ochrony prywatności. Obejmowało to zbadanie możliwości przyjęcia ustaleń z wybranymi

---

[54] Zob. globalne badanie CIGHI-Ipsos na temat bezpieczeństwa i zaufania w internecie z 2019 r. (*Global Survey on Internet Security and Trust 2019 CIGHI-Ipsos Global Survey*). Według tego badania 78 % respondentów wyraziło zaniepokojenie w związku ze swoją prywatnością w internecie, a 49 % z nich stwierdziło, że w związku z brakiem zaufania ujawnia mniej danych osobowych online; 43 % podejmuje większe starania w celu zabezpieczenia swoich urządzeń, a 39 % odpowiedziało, że wykorzystuje internet w sposób bardziej wybiórczy, oprócz innych środków ostrożności. Badanie przeprowadzono w 25 krajach: Australii, Brazylii, Kanadzie, Chinach, Egipcie, Francji, Niemczech, Wielkiej Brytanii, Hongkongu, Indiach, Indonezji, Włoszech, Japonii, Kenii, Meksyku, Nigerii, Pakistanie, Polsce, Rosji, Republice Południowej Afryki, Republice Korei, Szwecji, Tunezji, Turcji i Stanach Zjednoczonych.

[55] Konwencja Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) oraz Protokół dodatkowy z 2001 r. do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych (ETS nr 181). Jest to jedyny wiążący instrument wielostronny w dziedzinie ochrony danych. Ostatnio konwencję ratyfikowały m.in. Argentyna, Meksyk, Republika Zielonego Przylądka i Maroko.

[56] Protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) uzgodniony na 128. posiedzeniu Komitetu Ministrów w Elsinore (Dania) w dniach 17-18 maja 2018 r. Skonsolidowany tekst zaktualizowanej konwencji ETS nr 108 jest dostępny na stronie internetowej: https://rm.coe.int/16808ade9d.

[57] Komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", COM/2017/07 final.

państwami trzecimi dotyczących zapewnienia odpowiedniego stopnia ochrony[58]. Prace te przyniosły istotne rezultaty, w szczególności wejście w życie w lutym 2019 r. porozumienia między UE a Japonią o wzajemnej odpowiedniej ochronie danych, które stworzyło największy na świecie obszar swobodnego i bezpiecznego przepływu danych. Negocjacje z Koreą Południową w sprawie odpowiedniej ochrony danych są na zaawansowanym etapie; prowadzone są także prace przygotowawcze mające na celu zainicjowanie negocjacji w sprawie odpowiedniej ochrony danych z kilkoma krajami Ameryki Łacińskiej, takimi jak Chile czy Brazylia, w zależności od zakończenia trwających procesów legislacyjnych. Obiecujące postępy odnotowano również w niektórych częściach Azji, takich jak Indie, Indonezja i Tajwan, a także w regionie europejskiego sąsiedztwa wschodniego i południowego, co może otworzyć drogę do przyszłych decyzji stwierdzających odpowiedni stopień ochrony danych osobowych.

Jednocześnie Komisja z zadowoleniem przyjmuje fakt, że inne państwa, które wprowadziły instrumenty przekazywania danych podobne do instrumentów zapewniających odpowiedni stopień ochrony danych zawartych w rozporządzeniu, uznały, że zarówno UE, jak i państwa uznane przez UE za państwa o odpowiednim poziomie ochrony danych zapewniają wymagany poziom ochrony danych[59]. Dzięki temu istnieje możliwość stworzenia w przyszłości sieci państw, w których możliwy będzie swobodny przepływ danych.

Jednocześnie trwają intensywne prace z innymi państwami trzecimi, takimi jak Kanada, Nowa Zelandia, Argentyna i Izrael, aby zapewnić ciągłość decyzji stwierdzających odpowiedni stopień ochrony danych osobowych przyjętych na podstawie dyrektywy o ochronie danych z 1995 r. w ramach nowego rozporządzenia. Tymczasem Tarcza Prywatności UE-USA okazała się użytecznym narzędziem do zapewniania transatlantyckiego przepływu danych w oparciu o wysoki poziom ochrony; uczestniczy w niej ponad 4 700 przedsiębiorstw[60]. Jej coroczny przegląd gwarantuje, regularne kontrole prawidłowego funkcjonowania ram, a pojawiające się kwestie mogą zostać rozwiązane w odpowiednim czasie.

Ponieważ nie istnieje uniwersalne podejście do przepływu danych, Komisja współpracuje również z zainteresowanymi stronami i radą w celu wykorzystania pełnego potencjału narzędzi przewidzianych w rozporządzeniu w odniesieniu do międzynarodowego przekazywania danych. Dotyczy to takich narzędzi jak standardowe klauzule umowne, opracowanie systemów certyfikacji, kodeksów postępowania lub uzgodnień administracyjnych dla organów publicznych. W związku z tym Komisja jest zainteresowana wymianą doświadczeń i najlepszych praktyk z innymi systemami, w ramach których zdobyto konkretną wiedzę fachową w zakresie niektórych z tych narzędzi. Komisja rozważy

---

[58] Rozporządzenie stworzyło możliwość ustaleń dotyczących odpowiedniego stopnia ochrony danych również w odniesieniu do organizacji międzynarodowych, w ramach wysiłków UE na rzecz ułatwienia wymiany danych z takimi podmiotami.

[59] Jest to podejście przyjęte na przykład przez Argentynę, Kolumbię, Izrael i Szwajcarię.

[60] Oznacza to, że w ciągu pierwszych trzech lat istnienia Tarczy Prywatności uczestniczy w niej więcej przedsiębiorstw, niż w poprzednim systemie („Bezpiecznej przystani") po 13 latach funkcjonowania.

wykorzystanie uprawnień przyznanych na mocy rozporządzenia w odniesieniu do tych narzędzi przekazywania danych, w szczególności standardowych klauzul umownych.

Oprócz narzędzi czysto dwustronnych można również rozważyć, czy kraje o podobnych poglądach mogłyby ustanowić międzynarodowe ramy w tej dziedzinie, biorąc pod uwagę fakt, że przepływy danych są w coraz większym stopniu kluczowym elementem wymiany handlowej, komunikacji oraz interakcji społecznych. Instrument taki umożliwiłby swobodny przepływ danych między umawiającymi się stronami, przy jednoczesnym zapewnieniu wymaganego poziomu ochrony w oparciu o wspólne wartości i konwergencję systemów. Mógłby zostać opracowany na przykład w oparciu o zaktualizowaną konwencję ETS nr 108 lub czerpiąc inspirację z inicjatywy „swobodny przepływ danych godny zaufania" zainicjowanej przez Japonię na początku tego roku.

Rozwijanie nowych synergii między instrumentami handlu i instrumentami ochrony danych

Propagując konwergencję standardów ochrony danych na szczeblu międzynarodowym, Komisja jest również zdecydowana zwalczać protekcjonizm cyfrowy. W tym celu Komisja opracowała szczegółowe przepisy dotyczące przepływu danych i ochrony danych w umowach handlowych, które systematycznie przedstawia w swoich negocjacjach dwustronnych i wielostronnych, takich jak obecne rozmowy w ramach WTO w sprawie handlu elektronicznego. Te przepisy horyzontalne wykluczają czysto protekcjonistyczne środki, takie jak przymusowe wymogi dotyczące lokalizacji danych, a z drugiej strony zachowują autonomię regulacyjną stron w zakresie ochrony podstawowego prawa do ochrony danych.

Pomimo że dialogi na temat ochrony danych i negocjacje handlowe muszą odbywać się oddzielnie, mogą się jednak wzajemnie uzupełniać: porozumienie pomiędzy UE a Japonią o wzajemnej odpowiedniej ochronie danych jest najlepszym przykładem takiej synergii, która ułatwia wymianę handlową, a przez to zwiększa korzyści wynikające z umowy o partnerstwie gospodarczym. Ten rodzaj konwergencji, oparty na wspólnych wartościach i wysokich standardach oraz poparty skutecznym egzekwowaniem przepisów, stanowi najsolidniejszą podstawę do wymiany danych osobowych, a fakt ten jest coraz częściej uznawany przez naszych partnerów międzynarodowych[61]. Biorąc pod uwagę, że przedsiębiorstwa coraz częściej prowadzą działalność transgraniczną i wolą stosować podobne zestawy przepisów w całej swojej działalności gospodarczej na całym świecie, taka konwergencja przyczynia się do stworzenia środowiska sprzyjającego inwestycjom bezpośrednim, ułatwiającego wymianę handlową i zwiększającego zaufanie między partnerami handlowymi.

Ułatwianie wymiany informacji w celu zwalczania przestępczości i terroryzmu w oparciu o odpowiednie zabezpieczenia

Większa zgodność między systemami ochrony danych może również znacznie ułatwić bardzo potrzebną wymianę informacji między UE a zagranicznymi organami regulacyjnymi, policją i organami sądowymi, a tym samym przyczynić się do skuteczniejszej i szybszej współpracy

[61] Znalazło to odzwierciedlenie na przykład w odniesieniu do koncepcji „swobodnego przepływu danych godnego zaufania" w deklaracji przywódców grupy G-20 po szczycie w Osace: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

w zakresie egzekwowania prawa[62]. W tym celu Komisja rozważa skorzystanie z możliwości przyjmowania decyzji stwierdzającej odpowiedni stopień ochrony danych osobowych zgodnie z dyrektywą o ochronie danych w sprawach karnych w celu pogłębienia współpracy z kluczowymi partnerami w walce z przestępczością i terroryzmem. Ponadto umowa parasolowa między UE a USA[63], która weszła w życie w lutym 2017 r., może być stosowana jako wzór dla podobnych umów z innymi ważnymi partnerami w dziedzinie bezpieczeństwa.

Inne przykłady wskazujące na znaczenie wysokich standardów ochrony danych jako podstawy stabilnej współpracy organów ścigania z państwami trzecimi to przekazywanie danych dotyczących przelotu pasażera (PNR)[64] oraz wymiana informacji operacyjnych między Europolem a ważnymi partnerami międzynarodowymi. W związku z tym obecnie prowadzone są lub zostaną rozpoczęte negocjacje w sprawie umów międzynarodowych z kilkoma państwami południowego sąsiedztwa[65].

Solidne zabezpieczenia w zakresie ochrony danych będą również zasadniczym elementem wszelkich przyszłych umów w sprawie transgranicznego dostępu do dowodów elektronicznych w dochodzeniach, zarówno na szczeblu dwustronnym (umowa między UE a USA) jak i wielostronnym (drugi protokół dodatkowy do budapeszteńskiej konwencji Rady Europy o cyberprzestępczości)[66].

Propagowanie współpracy między organami odpowiedzialnymi za egzekwowanie przepisów w zakresie ochrony danych

W czasie, gdy kwestie związane z przestrzeganiem prawa do prywatności lub incydenty związane z bezpieczeństwem mogą mieć wpływ na dużą liczbę osób jednocześnie w kilku jurysdykcjach, bliższe formy współpracy między organami nadzoru na szczeblu międzynarodowym mogą pomóc w zapewnieniu zarówno skuteczniejszej ochrony praw indywidualnych, jak i bardziej stabilnego środowiska dla podmiotów gospodarczych. W tym kontekście i w ścisłej współpracy z radą Komisja będzie pracować nad sposobami ułatwienia współpracy w zakresie egzekwowania prawa i wzajemnej pomocy między unijnymi

---

62 Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Europejska agenda bezpieczeństwa, COM(2015) 185 final.

63 Umowa między UE a Stanami Zjednoczonymi w sprawie ochrony danych osobowych przekazywanych i przetwarzanych do celów działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych, w tym terroryzmu, w ramach współpracy policyjnej i sądowej w sprawach karnych: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22016A1210 („umowa parasolowa"). Umowa parasolowa stanowi pierwszą dwustronną umowę międzynarodową w dziedzinie egzekwowania prawa przewidującą kompleksowy katalog praw i obowiązków w zakresie ochrony danych zgodnie z unijnym dorobkiem prawnym. Jest to dobry przykład tego, w jaki sposób współpraca w zakresie egzekwowania prawa z ważnym partnerem międzynarodowym może zostać wzmocniona dzięki wynegocjowaniu solidnego zestawu zabezpieczeń w zakresie ochrony danych.

64 Rezolucja Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych nr 2396 z dnia 21 grudnia 2017 r. wzywa wszystkie państwa członkowskie ONZ do rozwijania zdolności do gromadzenia, przetwarzania i analizowania danych PNR przy pełnym poszanowaniu praw człowieka i podstawowych wolności. Zob. również komunikat Komisji „Europejska agenda bezpieczeństwa", COM (2015) 185 final: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52015DC0185&qid=1529484757152&from=EN.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

66 http://europa.eu/rapid/press-release_IP-19-2891_en.htm

i zagranicznymi organami nadzoru, w tym poprzez wykorzystanie nowych uprawnień przewidzianych w tym obszarze w rozporządzeniu[67]. Mogłoby to obejmować różne formy współpracy przy opracowywaniu interpretacyjnych lub praktycznych narzędzi[68] w celu wymiany informacji na temat toczących się dochodzeń.

Ponadto Komisja zamierza również zintensyfikować dialog z organizacjami i sieciami regionalnymi, takimi jak Stowarzyszenie Narodów Azji Południowo-Wschodniej (ASEAN), Unia Afrykańska, Forum organów ds. prywatności w regionie Azji i Pacyfiku (APPF) lub Iberoamerykańska sieć ochrony danych, które odgrywają coraz większą rolę w kształtowaniu wspólnych standardów ochrony danych, propagowaniu wymiany najlepszych praktyk oraz wspieraniu współpracy między organami odpowiedzialnymi za egzekwowanie prawa. Komisja będzie również współpracować z Organizacją Współpracy Gospodarczej i Rozwoju oraz Organizacją Współpracy Gospodarczej Azji i Pacyfiku w celu osiągnięcia konwergencji prowadzącej do wysokiego poziomu ochrony danych.

VII. Prawodawstwo w dziedzinie ochrony danych jako integralna część szerokiego zakresu polityk

Ochrona danych osobowych jest zagwarantowana w ramach szeregu polityk Unii i stanowi ich część.

Usługi telekomunikacyjne i elektroniczne

W styczniu 2017 r. Komisja przyjęła wniosek dotyczący rozporządzenia w sprawie prywatności i łączności elektronicznej[69]. Wniosek ten ma na celu ochronę poufności komunikacji, zgodnie z postanowieniami Karty praw podstawowych, ochronę danych osobowych, które mogą być częścią komunikacji, jak również ochronę urządzeń końcowych użytkowników końcowych.

Proponowane rozporządzenie w sprawie prywatności i łączności elektronicznej uszczegóławia i uzupełnia rozporządzenie poprzez ustanowienie szczegółowych przepisów dla wyżej wymienionych celów. Unowocześnia obecne unijne zasady dotyczące e-prywatności[70] w celu uwzględnienia zmian technologicznych i prawnych. Zwiększa także prywatność osób fizycznych poprzez rozszerzenie zakresu stosowania nowych przepisów na dostawców usług OTT, tworząc tym samym równe warunki działania dla wszystkich usług łączności elektronicznej. Parlament Europejski przyjął mandat do rozpoczęcia rozmów trójstronnych w październiku 2017 r., jednak Rada nie uzgodniła jeszcze podejścia ogólnego. Komisja pozostaje w pełni zaangażowana w rozporządzenie w sprawie prywatności

---

[67] Zob. art. 50 rozporządzenia w sprawie współpracy międzynarodowej w dziedzinie ochrony danych. Przepis ten obejmuje szeroki zakres form współpracy, od informacji na temat przepisów o ochronie danych, aż po przekazywanie skarg i pomoc w postępowaniu wyjaśniającym.

[68] Takie jak wspólne wzory powiadomień o naruszeniu ochrony danych.

[69] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

[70] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37-47.

i łączności elektronicznej i będzie wspierać współprawodawców w ich staraniach na rzecz szybkiego przyjęcia proponowanego rozporządzenia.

Zdrowie i badania

Ułatwienie wymiany danych dotyczących zdrowia, które stanowią dane wrażliwe na mocy rozporządzenia, między państwami członkowskimi staje się coraz ważniejsze w dziedzinie zdrowia publicznego ze względu na interes ogólny. Dotyczą one zapewnienia opieki zdrowotnej lub leczenia, ochrony przed poważnymi transgranicznymi zagrożeniami zdrowia oraz zapewnienia wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych i wyrobów medycznych. Rozporządzenie określa przepisy, które zapewniają legalne i godne zaufania metody przetwarzania i wymiany danych dotyczących zdrowia w całej UE. Przepisy te mają również zastosowanie do dostępu osób trzecich do danych medycznych pacjentów, w tym do danych przechowywanych w kartotekach pacjentów, e-recept i długoterminowej kompleksowej elektronicznej dokumentacji medycznej, a także do ich wykorzystywania do celów badań naukowych. W szczególnym obszarze badań klinicznych Komisja przygotowała również konkretny zestaw pytań i odpowiedzi na temat wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych[71] a ogólnym rozporządzeniem o ochronie danych[72].

Sztuczna inteligencja:

Ze względu na to, że sztuczna inteligencja ma znaczenie strategiczne, istotne jest określenie globalnych zasad jej rozwoju i wykorzystania. Promując rozwój i wdrażanie sztucznej inteligencji, Komisja wybrała podejście zorientowane na człowieka, co oznacza, że zastosowania sztucznej inteligencji muszą być zgodne z prawami podstawowymi[73]. W tym kontekście zasady określone w rozporządzeniu stanowią ogólne ramy i zawierają konkretne zobowiązania i prawa, które są szczególnie istotne w odniesieniu do przetwarzania danych osobowych przez sztuczną inteligencję. Rozporządzenie obejmuje m.in. prawo do tego, by nie podlegać wyłącznie zautomatyzowanemu podejmowaniu decyzji, z wyjątkiem niektórych sytuacji[74]. Zawiera ono również szczegółowe wymogi w zakresie przejrzystości w odniesieniu do zautomatyzowanego podejmowania decyzji, a mianowicie obowiązek informowania o istnieniu takich decyzji oraz obowiązek dostarczenia istotnych informacji i wyjaśnienia ich

---

71 https://eur-lex.europa.eu/legal-content/PLXT/?uri=celex%3A32014R0536

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

73 Komunikat Komisji z dnia 8 kwietnia 2019 r. w sprawie budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji przedstawione przez grupę ekspertów wysokiego szczebla w dniu 8 kwietnia 2019 r.: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Zob. również zalecenie Rady OECD w sprawie sztucznej inteligencji: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, zasady grupy G20 dotyczące sztucznej inteligencji zatwierdzone w ramach deklaracji przywódców grupy G20 po szczycie w Osace: https://www.g20.org/pdf/documents/en/annex_08.pdf oraz deklaracja ministrów grupy G20 w sprawie handlu i gospodarki cyfrowej: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

74 Art. 22 rozporządzenia.

znaczenia oraz przewidywanych konsekwencji przetwarzania dla danej osoby[75]. Te podstawowe zasady rozporządzenia zostały uznane przez grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji[76], Organizację Współpracy Gospodarczej i Rozwoju[77] oraz grupę G20[78] za szczególnie istotne w kontekście wyzwań i możliwości związanych ze sztuczną inteligencją. Europejska Rada Ochrony Danych wskazała sztuczną inteligencję jako jeden z możliwych tematów w swoim programie prac na lata 2019–2020[79].

Sektor transportu

Rozwój samochodów podłączonych do sieci i inteligentnych miast w coraz większym stopniu polega na przetwarzaniu dużych ilości danych osobowych i ich wymianie między różnymi stronami, w tym pomiędzy samochodami, ich producentami, dostawcami usług telematycznych oraz organami publicznymi odpowiedzialnymi za infrastrukturę drogową. To wielostronne otoczenie pociąga za sobą pewną złożoność w odniesieniu do podziału ról i obowiązków poszczególnych podmiotów zaangażowanych w przetwarzanie danych osobowych oraz na temat tego, w jaki sposób zapewnić zgodność z prawem przetwarzania danych przez wszystkie te podmioty. Zapewnienie zgodności z rozporządzeniem oraz prawodawstwo w dziedzinie prywatności i łączności elektronicznej mają zasadnicze znaczenie dla skutecznego wdrożenia inteligentnych systemów transportowych we wszystkich rodzajach transportu, a także dla rozpowszechniania cyfrowych narzędzi i usług umożliwiających większą mobilność osób i towarów[80].

Energia

Rozwój rozwiązań cyfrowych w sektorze energetycznym w coraz większym stopniu polega na przetwarzaniu danych osobowych. Akty prawne przyjęte w ramach pakietu „Czysta energia dla wszystkich Europejczyków”[81] zawierają nowe przepisy umożliwiające cyfryzację sektora energii elektrycznej oraz przepisy dotyczące dostępu do danych, zarządzania nimi i ich interoperacyjności, które umożliwiają przetwarzanie danych konsumentów w czasie rzeczywistym w celu uzyskiwania przez nich korzyści oraz zachęcania ich do własnej produkcji energii i uczestnictwa w rynku energii. W związku z tym zapewnienie zgodności z przepisami o ochronie danych ma ogromne znaczenie dla pomyślnego wdrożenia tych przepisów.

---

75 Art. 13 ust. 2 lit. f) rozporządzenia.

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

77 Zalecenie Rady w sprawie sztucznej inteligencji: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

78 Deklaracja ministrów grupy G20 w sprawie handlu i gospodarki cyfrowej: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_pl.pdf

80 Na przykład poprzez ułatwienie planowania i korzystania z różnych środków transportu podczas podróży lub przewozu.

81 W szczególności dyrektywa w sprawie energii elektrycznej: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32009L0072.

Konkurencja

Przetwarzanie danych osobowych w coraz większym stopniu stanowi element, który należy uwzględnić w polityce konkurencji[82]. Biorąc pod uwagę, że organy odpowiedzialne za ochronę danych są jedynymi organami, którym powierzono przeprowadzenie oceny naruszenia przepisów dotyczących ochrony danych, organy ochrony konkurencji, konsumentów oraz organy ochrony danych współpracują ze sobą i będą nadal współpracować w stosownych przypadkach na styku swoich kompetencji. Komisja będzie wspierać taką współpracę i uważnie śledzić rozwój wydarzeń.

Kontekst wyborczy

W wytycznych dotyczących wykorzystania danych osobowych w kontekście wyborczym[83], wydanych we wrześniu 2018 r. jako część pakietu dotyczącego wyborów[84], Komisja zwróciła uwagę na zasady mające szczególne znaczenie dla podmiotów biorących udział w wyborach, w tym na kwestie dotyczące tzw. „mikrotargetingu wyborców". Podobne stanowisko zostało wyrażone w oświadczeniu Europejskiej Rady Ochrony Danych[85], a szereg organów ochrony danych wydało wytyczne na szczeblu krajowym. Pakiet dotyczący wyborów obejmował również wezwanie każdego państwa członkowskiego do utworzenia krajowej sieci wyborczej (z udziałem organów krajowych odpowiedzialnych za sprawy wyborcze oraz organów odpowiedzialnych za monitorowanie i egzekwowanie przepisów, takich jak ochrona danych) dotyczącej działalności online istotnej z punktu widzenia wyborów. Przyjęto również nowe środki w celu wprowadzenia sankcji za naruszenia przepisów o ochronie danych przez europejskie partie i fundacje polityczne. Komisja zaleciła państwom członkowskim przyjęcie takiego samego podejścia na szczeblu krajowym. Ocena wyborów do Parlamentu Europejskiego w 2019 r., która ma zostać wydana w październiku 2019 r., uwzględni również aspekty ochrony danych.

Egzekwowanie prawa

Skuteczna i rzeczywista unia bezpieczeństwa może opierać się wyłącznie na pełnym przestrzeganiu praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej oraz w prawie wtórnym UE, w tym na zapewnieniu odpowiednich zabezpieczeń w zakresie ochrony danych w celu umożliwienia bezpiecznej wymiany danych osobowych do celów egzekwowania prawa. Wszelkie ograniczenia podstawowego prawa do prywatności i ochrony danych podlegają testowi ścisłej konieczności i proporcjonalności.

---

82 Na przykład sprawa M.8788 – Apple / Shazam oraz sprawa M.8124 – Microsoft / LinkedIn.

83 https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

84 http://europa.eu/rapid/press-release_IP-18-5681_pl.htm

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

VIII. Podsumowanie

Na podstawie dostępnych dotychczas informacji i dialogu z zainteresowanymi stronami Komisja dokonała wstępnej oceny, zgodnie z którą pierwszy rok stosowania rozporządzenia był ogólnie pozytywny. Niemniej jednak, jak wykazano w niniejszym komunikacie, w wielu obszarach konieczne są dalsze postępy.

Wdrażanie i uzupełnianie ram prawnych:

- Trzy państwa członkowskie, które jeszcze nie zaktualizowały swoich krajowych przepisów o ochronie danych, muszą to zrobić w trybie pilnym. Wszystkie państwa członkowskie powinny zakończyć dostosowanie swojego ustawodawstwa sektorowego do wymogów rozporządzenia.

- Komisja wykorzysta wszystkie dostępne jej narzędzia, w tym postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, aby zapewnić przestrzeganie przez państwa członkowskie przepisów rozporządzenia oraz ograniczyć ryzyko fragmentacji ram ochrony danych.

Pełne wykorzystanie potencjału nowego systemu zarządzania:

- Państwa członkowskie powinny przydzielić krajowym organom ochrony danych wystarczające zasoby ludzkie, finansowe i techniczne.

- Organy ochrony danych powinny zacieśnić współpracę, na przykład poprzez prowadzenie wspólnych dochodzeń. Państwa członkowskie powinny ułatwiać prowadzenie takich dochodzeń.

- Rada powinna dalej rozwijać unijną kulturę ochrony danych i w pełni wykorzystywać narzędzia przewidziane w rozporządzeniu, aby zapewnić jednolite stosowanie przepisów. Powinna także kontynuować prace nad wytycznymi, zwłaszcza dla małych i średnich przedsiębiorstw.

- Należy zwiększyć wiedzę ekspercką sekretariatu rady w celu wspierania rady i skuteczniejszego prowadzenia jej prac.

- Komisja będzie nadal wspierać organy ochrony danych i radę, w szczególności poprzez aktywny udział w pracach rady i zwracanie uwagi na wymogi prawa UE w procesie wdrażania rozporządzenia.

- Komisja będzie wspierać kontakty między organami ochrony danych a innymi organami, zwłaszcza z obszaru konkurencji, z pełnym poszanowaniem ich odpowiednich kompetencji.

Wspieranie i angażowanie zainteresowanych stron:

- Rada powinna usprawnić sposób, w jaki angażuje zainteresowane strony w swoje prace. Komisja będzie nadal udzielać wsparcia finansowego organom ochrony danych, aby pomóc im dotrzeć do zainteresowanych stron.

- Komisja będzie kontynuować działania informacyjne i współpracować z zainteresowanymi stronami.

Promowanie międzynarodowej konwergencji:

- Komisja będzie w dalszym ciągu intensyfikować dialog w kwestii odpowiedniości ochrony z kwalifikującymi się kluczowymi partnerami, w tym w obszarze egzekwowania prawa. Komisja ma w szczególności na celu zakończenie w nadchodzących miesiącach trwających negocjacji z Koreą Południową. W 2020 r. Komisja przedstawi sprawozdanie na temat przeglądu 11 decyzji stwierdzających odpowiedni stopień ochrony danych osobowych, przyjętych na podstawie dyrektywy o ochronie danych.

- Komisja będzie kontynuować swoje prace, w tym poprzez wymianę informacji i najlepszych praktyk w zakresie pomocy technicznej, z państwami zainteresowanymi przyjęciem nowoczesnych przepisów dotyczących prywatności, a także wspierać współpracę z organami nadzoru i organizacjami regionalnymi z państw trzecich.

- Komisja będzie współpracować z organizacjami wielostronnymi i regionalnymi w celu promowania wysokich standardów ochrony danych jako czynnika ułatwiającego wymianę handlową oraz ułatwiającego współpracę (np. w ramach inicjatywy „swobodnego przepływu danych godnego zaufania" zainicjowanej przez Japonię w kontekście grupy G20).

Rozporządzenie[86] nakłada na Komisję obowiązek złożenia sprawozdania z jego wdrożenia w 2020 r. Będzie to okazja do oceny poczynionych postępów oraz tego, czy po dwóch latach stosowania poszczególne elementy nowego systemu ochrony danych są w pełni operacyjne. W tym celu Komisja będzie współpracować z Parlamentem Europejskim, Radą, państwami członkowskimi, Europejską Radą Ochrony Danych oraz odpowiednimi zainteresowanymi stronami i obywatelami.

[86] Art. 97 rozporządzenia.