KOMISJA
EUROPEJSKA

Bruksela, dnia 24.6.2020 r.
COM(2020) 264 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych

{SWD(2020) 115 final}

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejście UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych

1 PRZEPISY O OCHRONIE DANYCH JAKO FILAR WZMACNIANIA POZYCJI OBYWATELI ORAZ PODEJŚCIE UE DO TRANSFORMACJI CYFROWEJ

Niniejsze sprawozdanie jest pierwszym sprawozdaniem z oceny i przeglądu ogólnego rozporządzenia o ochronie danych[1] (zwanego dalej „RODO"), w szczególności w odniesieniu do stosowania i funkcjonowania przepisów dotyczących przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych oraz przepisów dotyczących współpracy i spójności zgodnie z art. 97 RODO.

Ogólne rozporządzenie o ochronie danych (RODO), które obowiązuje od dnia 25 maja 2018 r., stanowi centralny element unijnych ram[2] gwarantujących podstawowe prawo do ochrony danych, zapisane w Karcie praw podstawowych Unii Europejskiej (art. 8) i w traktatach (art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, „TFUE"). Dzięki wprowadzeniu RODO wzmocniono gwarancje ochrony danych, zapewniono obywatelom dodatkowe i większe prawa oraz większą przejrzystość, a także zagwarantowano, że wszystkie podmioty wykorzystujące dane osobowe objęte zakresem stosowania tego rozporządzenia podlegają większej odpowiedzialności. W rozporządzeniu tym wyposażono niezależne organy ochrony danych w większe i zharmonizowane uprawnienia w zakresie egzekwowania prawa oraz ustanowiono nowy system zarządzania. Ustanowiono w nim także równe warunki działania dla wszystkich przedsiębiorstw działających na rynku UE, niezależnie od miejsca ich siedziby, oraz zapewniono swobodny przepływ danych w UE, wzmacniając tym samym rynek wewnętrzny.

RODO jest ważnym elementem ukierunkowanego na człowieka podejścia do technologii i jednocześnie nadaje kierunek w wykorzystywaniu technologii w transformacji ekologicznej i cyfrowej, które charakteryzują kształtowanie polityki UE. Zostało to ostatnio podkreślone w białej księdze w sprawie sztucznej inteligencji[3]

---

[1] Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz.U. L 119 z 4.5.2016, s. 1.

[2] Po włączeniu go do Porozumienia o Europejskim Obszarze Gospodarczym (EOG) rozporządzenie stosuje się również do Norwegii, Islandii i Liechtensteinu.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

i w komunikacie w sprawie europejskiej strategii w zakresie danych[4] (zwanej dalej „strategią w zakresie danych") z lutego 2020 r.

W gospodarce, która w coraz większym stopniu opiera się na przetwarzaniu danych, w tym danych osobowych, RODO stanowi istotne narzędziem gwarantujące, że osoby fizyczne mają większą kontrolę nad swoimi danymi osobowymi i że dane te są przetwarzane do celów zgodnych z prawem, w sposób legalny, uczciwy i przejrzysty. Jednocześnie RODO przyczynia się do wspierania godnych zaufania innowacji, zwłaszcza dzięki podejściu opartym na analizie ryzyka i zasadom takim jak uwzględnianie ochrony prywatności już w fazie projektowania oraz domyślna ochrona prywatności. Komisja zaproponowała uzupełnienie ram prawnych dotyczących ochrony danych i prywatności[5] za pomocą rozporządzenia o prywatności i łączności elektronicznej[6], które ma zastąpić obecną dyrektywę o prywatności i łączności elektronicznej[7]. Wniosek ten jest obecnie analizowany przez współprawodawców i jego szybkie przyjęcie jest bardzo istotne.

W ramach priorytetów Komisji w zakresie „Europy na miarę ery cyfrowej"[8] i „Europejskiego Zielonego Ładu"[9] można opracować nowe inicjatywy umożliwiające obywatelom odgrywanie bardziej aktywnej roli w transformacji cyfrowej oraz w wykorzystywaniu narzędzi cyfrowych w dążeniu do społeczeństwa neutralnego dla klimatu i do bardziej zrównoważonego rozwoju. W RODO ustanowiono ramy dla tych inicjatyw i zagwarantowano, że mają one na celu skuteczne wzmocnienie pozycji osób fizycznych.

W ramach strategii w zakresie danych[10] wezwano do utworzenia „wspólnej europejskiej przestrzeni danych", prawdziwie jednolitego rynku danych, a także dziesięciu wspólnych europejskich sektorowych przestrzeni danych istotnych w kontekście transformacji ekologicznej i cyfrowej[11]. Dla wszystkich tych priorytetów kluczowe znaczenie mają jasne i wykonalne ramy wymiany danych i zwiększenia dostępności danych. W ramach strategii w zakresie danych ogłoszono również zamiar zbadania przez Komisję w przyszłym prawodawstwie, w jaki sposób należałoby

---

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pl

[5] Te ramy prawne obejmują również dyrektywę o ochronie danych w sprawach karnych (dyrektywę 2016/680) oraz rozporządzenie o ochronie danych w odniesieniu do instytucji i organów UE (rozporządzenie 2018/1725).

[6] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final – 2017/03(COD).

[7] 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.

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pl

[9] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Europejski Zielony Ład (COM(2019) 640 final).

[10] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Europejska strategia w zakresie danych", COM(2020) 66 final.

[11] Przestrzenie sektorowe obejmują takie obszary jak: zdrowie, produkcja przemysłowa, energia, mobilność, rolnictwo, dane finansowe, administracja publiczna, wspólny europejski obszar danych dotyczących umiejętności, wspólna europejska przestrzeń danych dotyczących Zielonego Ładu oraz europejska chmura dla otwartej nauki.

umożliwić wykorzystanie danych przechowywanych w publicznych bazach danych do celów badań naukowych w sposób zgodny z RODO. Przestrzenie danych mają być wspierane przez europejską federację chmury obliczeniowej, co zapewni przetwarzanie danych i usługi w zakresie infrastruktury chmury obliczeniowej w zgodzie z RODO. RODO zapewnia wysoki poziom ochrony danych osobowych i centralną rolę osób fizycznych we wszystkich tych przestrzeniach danych, zapewniając jednocześnie niezbędną elastyczność umożliwiającą uwzględnienie różnych podejść.

Potrzeba zapewnienia zaufania i zapotrzebowania na ochronę danych osobowych z pewnością nie jest ograniczona do UE. Osoby fizyczne na całym świecie w coraz większym stopniu doceniają prywatność i bezpieczeństwo swoich danych. Jak wykazano w ramach niedawno przeprowadzanego badania globalnego[12], uważają one, że jest to istotny czynnik wpływający na ich decyzje dotyczące zakupu i zachowania w internecie. Rosnąca liczba przedsiębiorstw odpowiada na to zapotrzebowanie na prywatność, na przykład przez dobrowolne rozszerzanie zakresu niektórych praw i zabezpieczeń przewidzianych w RODO na ich klientów spoza UE. Wiele przedsiębiorstw propaguje również poszanowanie danych osobowych jako element przewagi konkurencyjnej i mocny atut na światowym rynku, oferując innowacyjne produkty i usługi za pomocą nowatorskich rozwiązań w zakresie prywatności lub bezpieczeństwa danych. Ponadto zwiększenie zdolności podmiotów sektora prywatnego i publicznego do gromadzenia i przetwarzania danych na dużą skalę nasuwa ważne i złożone pytania, które w coraz większym stopniu stawiają prywatność w centrum debaty publicznej w różnych częściach świata.

Przyjęcie ogólnego rozporządzenia o ochronie danych przyczyniło się do tego, że inne państwa w wielu regionach świata również podjęły działania w tej kwestii. Jest to prawdziwie globalny trend, począwszy od Chile po Koreę Południową, od Brazylii po Japonię, od Kenii po Indie oraz od Kalifornii po Indonezję. Przywództwo UE w dziedzinie ochrony danych pokazuje, że może ona działać jako globalny organ normalizacyjny w odniesieniu do regulacji gospodarki cyfrowej; fakt ten został pozytywnie przyjęty przez ważnych członków społeczności międzynarodowej, takich jak sekretarz generalny ONZ António Guterres, który stwierdził, że RODO daje „dobry przykład, […] który inspiruje do podejmowania podobnych działań w innych częściach świata", oraz zaapelował „do UE i jej państw członkowskich, by nadal prowadziły do kształtowania ery cyfrowej i odgrywały wiodącą rolę w zakresie innowacji technologicznych i regulacji.[13]

Obecny kryzys związany z COVID-19 stanowi żywy obraz tej globalizacji debaty na temat ochrony prywatności zarówno w czasie kryzysu, jak i w kontekście przyszłego świata po wyjściu z niego. Kilka państw członkowskich UE podjęło działania nadzwyczajne w celu ochrony zdrowia publicznego. RODO wyraźnie podkreśla, że

---

[12] Zob. np. badanie na temat prywatności konsumentów Cisco 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Według tego badania obejmującego ankietę przeprowadzoną wśród 2 600 konsumentów na całym świecie duże grono konsumentów podjęło już działania w celu ochrony swojej prywatności, na przykład zmieniając firmę lub dostawców ze względu na ich politykę w zakresie danych lub praktyki w zakresie wymiany danych.

[13] Przemówienie Sekretarza Generalnego ONZ w Senacie Włoch, 18 grudnia 2019 r. (dokument dostępny na stronie: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

wszelkie ograniczenia muszą być zgodne z istotą podstawowych praw i wolności oraz być środkiem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, który służy do celów ochrony interesu publicznego takiego jak zdrowie publiczne. W związku z tym, że środki izolacji są stopniowo znoszone, decydenci muszą odpowiedzieć na oczekiwania obywateli co do oferty rozwiązań cyfrowych, które są godne zaufania i respektują prawa do prywatności i ochrony danych osobowych.

W wielu krajach wbudowane w system środki ochrony prywatności, takie jak dobrowolne zapisywanie się przez użytkowników, minimalizacja danych i ochrona danych, a także wyłączenie geolokalizacji, uznaje się za niezbędne do zapewnienia wiarygodności i społecznej akceptacji rozwiązań opartych na danych mających na celu monitorowanie i ograniczenie rozprzestrzeniania się wirusa, kalibrację środków przeciwdziałania w zakresie polityki publicznej, pomoc pacjentom lub wdrażanie strategii wyjścia. W UE ramy prawne dotyczące ochrony danych i prywatności[14] okazały się wystarczająco elastycznym narzędziem umożliwiającym opracowanie praktycznych rozwiązań (np. aplikacji do śledzenia kontaktów) przy jednoczesnym zapewnieniu wysokiego poziomu ochrony danych osobowych. W tym kontekście w dniu 16 kwietnia 2020 r. Komisja opublikowała wytyczne dotyczące aplikacji wspierających walkę z pandemią w odniesieniu do ochrony danych[15].

Ochrona danych osobowych ma również zasadnicze znaczenie dla zapobiegania manipulacjom w zakresie wyborów dokonywanych przez obywateli, w szczególności poprzez mikrotargetowanie wyborców w oparciu o niezgodne z prawem przetwarzanie danych osobowych, unikanie ingerencji w procesy demokratyczne oraz zachowanie otwartej debaty, sprawiedliwości i przejrzystości, które są niezbędne w demokracji. Z tego względu we wrześniu 2018 r. Komisja opublikowała wytyczne w sprawie stosowania unijnych przepisów o ochronie danych w kontekście wyborczym[16].

W ramach tej oceny i przeglądu Komisja wzięła pod uwagę wkład Rady[17], Parlamentu Europejskiego[18], Europejskiej Rady Ochrony Danych (zwanej dalej „EROD")[19] oraz indywidualnych organów ochrony danych[20], grupy ekspertów

---

[14] Ramy te, oprócz RODO, obejmują dyrektywę o prywatności i łączności elektronicznej (dyrektywa 2002/58/WE), która obejmuje m.in. przepisy dotyczące dostępu do informacji na temat urządzeń końcowych użytkownika i przechowywania takich informacji.

[15] Komunikat Komisji zatytułowany „Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych", 2020/C 124 I/01 – C/2020/2523 – Dz.U. C 124I z 17.4.2020, s. 1. W dniu 16 kwietnia 2020 r. państwa członkowskie UE, przy wsparciu Komisji, opracowały zestaw narzędzi UE na potrzeby wykorzystywania aplikacji mobilnych do śledzenia kontaktów i ostrzegania w odpowiedzi na pandemię koronawirusa. Jest to część wspólnego skoordynowanego podejścia mającego na celu wspieranie stopniowego znoszenia środków izolacji. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Wytyczne Komisji dotyczące stosowania unijnych przepisów o ochronie danych osobowych w kontekście wyborczym – wkład Komisji Europejskiej na spotkanie przywódców w Salzburgu w dniach 19–20 września 2018 r. - COM(2018) 638 final.

[17] Stanowisko Rady i ustalenia w sprawie stosowania ogólnego rozporządzenia o ochronie danych: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/pl/pdf.

[18] Pismo Komisji LIBE Parlamentu Europejskiego z dnia 21 lutego 2020 r. skierowane do komisarza Reyndersa, nr ref.: IPOL-COM-LIBE D (2020)6525.

[19] Wkład EROD w ocenę ogólnego rozporządzenia o ochronie danych na mocy art. 97, przyjęty w dniu 18 lutego 2020 r.: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_pl.

z udziałem wielu zainteresowanych stron[21] i innych zainteresowanych stron, w tym informacje zwrotne przekazane w odniesieniu do planu działania[22].

Ogólny pogląd jest taki, że dwa lata po wejściu w życie RODO z powodzeniem realizuje swoje cele polegające na wzmocnieniu ochrony prawa jednostki do ochrony danych osobowych i zagwarantowaniu swobodnego przepływu danych osobowych w UE [23]. Stwierdzono jednak również szereg obszarów, w których można by wprowadzić pewne ulepszenia. Podobnie jak większość zainteresowanych stron i organów ochrony danych Komisja jest zdania, że na obecnym etapie przedwczesne byłoby wyciąganie ostatecznych wniosków dotyczących stosowania RODO. Jest prawdopodobne, że przy rozwiązywaniu większości problemów wskazanych przez państwa członkowskie i zainteresowane strony będzie pomoże większe doświadczenie w stosowaniu RODO w nadchodzących latach. Niemniej jednak w niniejszym sprawozdaniu przedstawiono wyzwania napotkane do tej pory przy stosowaniu RODO oraz możliwe sposoby rozwiązania tych problemów.

Poza skupieniem się na dwóch kwestiach, o których mowa w art. 97 ust. 2 RODO, a mianowicie na przekazywaniu danych osobowych do państw trzecich lub organizacji międzynarodowych oraz na mechanizmach współpracy i spójności, w ramach tej oceny i przeglądu przyjęto również szersze podejście do kwestii poruszonych przez różne podmioty w ciągu ostatnich dwóch lat.

2 GŁÓWNE WNIOSKI

Egzekwowanie RODO oraz funkcjonowanie mechanizmu współpracy i spójności

W ramach RODO ustanowiono innowacyjny system zarządzania w oparciu o niezależne organy ochrony danych w państwach członkowskich i ich współpracę w sprawach transgranicznych oraz w ramach Europejskiej Rady Ochrony Danych („EROD"). Ogólnie uważa się, że organy ochrony danych w sposób zrównoważony wykorzystały swoje wzmocnione uprawnienia naprawcze, w tym ostrzeżenia i upomnienia, grzywny oraz ograniczenia czasowe lub definitywne dotyczące przetwarzania danych[24]. Komisja zauważa, że organy stosowały kary administracyjne wynoszące od kilku tysięcy do kilku milionów euro, w zależności od wagi naruszeń. Inne sankcje, takie jak zakaz przetwarzania danych, mogą wywołać taki sam, jeżeli nie większy, efekt odstraszający, co grzywny. Ostatecznym celem RODO jest zmiana kultury i zachowania wszystkich zaangażowanych podmiotów z korzyścią dla obywateli. Bardziej szczegółowe informacje na temat wykorzystania uprawnień naprawczych przez organy ochrony danych przedstawiono w towarzyszącym dokumencie roboczym służb Komisji.

---

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_pl

[21] Utworzona przez Komisję wielostronna grupa ekspertów ds. rozporządzenia 2016/679 obejmuje przedstawicieli społeczeństwa obywatelskiego i przedsiębiorców, pracowników akademickich i praktyków: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Zob. np. stanowisko i ustalenia Rady oraz wkład EROD.

[24] Zob. pkt 2.1 dokumentu roboczego służb Komisji.

Choć wciąż jest zbyt wcześnie na pełną ocenę funkcjonowania nowych mechanizmów współpracy i spójności, organy ochrony danych zacieśniły współpracę poprzez mechanizm kompleksowej obsługi[25] i szerokie wykorzystanie wzajemnej pomocy[26]. Mechanizm kompleksowej obsługi, który jest kluczowym atutem rynku wewnętrznego, jest wykorzystywany do rozstrzygania wielu spraw transgranicznych[27]. Obecnie trwają prace nad ważnymi decyzjami o wymiarze transgranicznym, które będą podlegać mechanizmowi kompleksowej obsługi. Decyzje te, dotyczące często wielonarodowych korporacji działających w sektorze zaawansowanych technologii, będą miały znaczny wpływ na prawa obywateli w wielu państwach członkowskich.

Rozwijanie prawdziwie wspólnej europejskiej kultury ochrony danych między organami ochrony danych jest jednak nadal procesem w toku. Organy ochrony danych nie wykorzystały jeszcze w pełni narzędzi przewidzianych w RODO, takich jak wspólne operacje, które mogą prowadzić do wspólnych dochodzeń. W niektórych przypadkach nie udało się osiągnąć wspólnego podejścia, które oznaczałoby przejście do najmniejszego wspólnego mianownika, a co za tym idzie – możliwości większej harmonizacji[28].

Konieczne są dalsze postępy prac, aby usprawnić i ujednolicić rozpatrywanie spraw transgranicznych w całej UE, w tym z proceduralnego punktu widzenia, na przykład w kwestiach takich jak procedury rozpatrywania skarg, kryteria dopuszczalności skarg, czas trwania postępowań w kontekście różnych ram czasowych lub brak odnośnych terminów w zakresie krajowego administracyjnego prawa procesowego, moment w postępowaniu, w którym przysługuje prawo do bycia wysłuchanym lub informacje i zaangażowanie skarżących w toku postępowania. Proces refleksji zainicjowany przez EROD w związku z powyższym został pozytywnie przyjęty, a Komisja bierze czynny udział w odnośnych dyskusjach[29].

Działania i wytyczne EROD mają kluczowe znaczenie dla dalszego spójnego rozwoju wymiany informacji między radą a zainteresowanymi stronami[30]. Do końca 2019 r. EROD przyjął 67 dokumentów, w tym 10 nowych wytycznych[31] oraz 43 opinii[32]. Zainteresowane strony zasadniczo z zadowoleniem przyjmują wytyczne EROD i zwracają się o dodatkowe wytyczne w odniesieniu do kluczowych pojęć zawartych

---

[25] Jeżeli dane przedsiębiorstwo przetwarza dane poza granicami jednego państwa, to właściwym organem ochrony danych jest jedno z państw członkowskich, w którym znajduje się główna siedziba spółki.

[26] Zob. pkt 2.2 dokumentu roboczego służb Komisji.

[27] W okresie od dnia 25 maja 2018 r. do dnia 31 grudnia 2019 r. w ramach procedury kompleksowej obsługi przedłożono 141 projektów decyzji, z czego 79 skutkowało wydaniem ostatecznych decyzji.

[28] Na przykład krajowe wykazy rodzajów operacji przetwarzania, które wymagają oceny skutków w zakresie ochrony danych na podstawie art. 35 RODO, mogłyby zostać bardziej zharmonizowane.

[29] Zob. pkt 2.2 dokumentu roboczego służb Komisji.

[30] W szczególności przedstawicielami przedsiębiorstw i społeczeństwa obywatelskiego. Zob. pkt 2.3 dokumentu roboczego służb Komisji.

[31] Są one uzupełnieniem 10 wytycznych przyjętych przez Grupę Roboczą Art. 29 w okresie poprzedzającym rozpoczęcie stosowania rozporządzenia i zatwierdzonych przez EROD. Między styczniem a końcem maja 2020 r. EROD przyjął również dodatkowe 4 wytyczne i dokonał aktualizacji istniejących wcześniej wytycznych.

[32] 42 z tych opinii przyjęto na podstawie art. 64 RODO, a jedna została przyjęta na podstawie art. 70 ust. 1 lit. s) RODO i dotyczyła decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Japonii.

w ogólnym rozporządzeniu o ochronie danych, ale również wskazują na niespójność między wytycznymi krajowymi a wytycznymi EROD. Podkreślają one potrzebę bardziej praktycznych porad, w szczególności bardziej konkretnych przykładów, oraz potrzebę wyposażenia organów ochrony danych w niezbędne zasoby ludzkie, techniczne i finansowe w celu skutecznego wykonywania ich zadań.

Komisja konsekwentnie podkreślała spoczywający na państwach członkowskich obowiązek przeznaczania wystarczających zasobów ludzkich, finansowych i technicznych na potrzeby krajowych organów ochrony danych[33]. Większość organów zanotowała wzrost liczby personelu i zwiększenie budżetu w latach 2016–2019[34], przy czym władze Irlandii, Niderlandów, Islandii, Luksemburga i Finlandii zanotowały największy względny wzrost liczby personelu. Ponieważ największe międzynarodowe korporacje technologiczne mają siedzibę w Irlandii i Luksemburgu, organy ochrony danych z tych państw działają jako organy wiodące w wielu ważnych sprawach transgranicznych i mogą potrzebować większych zasobów niż wynikałoby to z liczby ludności. Sytuacja jest jednak nadal nierówna między państwami członkowskimi i w ujęciu ogólnym nie można tego stanu uznać za zadowalający. Organy ochrony danych odgrywają zasadniczą rolę w zapewnieniu egzekwowania RODO na szczeblu krajowym oraz skutecznego funkcjonowania mechanizmów współpracy i spójności w ramach EROD, w tym w szczególności mechanizmu kompleksowej obsługi w sprawach transgranicznych. W związku z tym wzywa się państwa członkowskie do zapewnienia im odpowiednich zasobów zgodnie z wymogami RODO[35].

Zharmonizowane przepisy przy istniejącym wciąż pewnym stopniu rozdrobnieniu i rozbieżnych podejściach

Komisja monitoruje wdrażanie RODO w przepisach krajowych. W momencie sporządzania niniejszego sprawozdania wszystkie państwa członkowskie, z wyjątkiem Słowenii, przyjęły nowe przepisy lub dostosowały własne krajowe przepisy o ochronie danych. Słowenia[36] została poproszona o przedstawienie Komisji wyjaśnień dotyczących zakończenia tego procesu[37].

W ramach RODO przewidziano spójne podejście do przepisów o ochronie danych w całej UE. Rozporządzenie nakłada jednak na państwa członkowskie obowiązek stanowienia prawa w niektórych obszarach[38] i daje im możliwość dalszego doprecyzowania RODO[39]. W związku z tym nadal istnieje pewien stopień fragmentacji, który wynika w szczególności z szerokiego zastosowania opcjonalnych klauzul precyzujących. Na przykład różnice między państwami członkowskimi w zakresie wieku wyrażenia zgody przez dzieci w odniesieniu do usług społeczeństwa

[33] Komunikat Komisji do Parlamentu Europejskiego i Rady, „Przepisy dotyczące ochrony danych jako czynnik sprzyjający zaufaniu w UE i poza nią – podsumowanie", COM(2019) 374 final z 24.7.2019.
[34] W latach 2016–2019 odnotowano łączny wzrost liczby personelu o 42 % oraz wzrost budżetu krajowych organów ochrony danych w EOG o 49 %.
[35] Zob. pkt 2.4 dokumentu roboczego służb Komisji.
[36] W ostatnim czasie za pośrednictwem pisma komisarza Reyndersa w marcu 2020 r.
[37] Należy zauważyć, że krajowy organ ochrony danych w Słowenii został ustanowiony na podstawie obowiązującego krajowego prawa o ochronie danych i nadzoruje stosowanie RODO w tym państwie członkowskim.
[38] Zob. pkt 3.1 dokumentu roboczego służb Komisji.
[39] Zob. pkt 3.2 dokumentu roboczego służb Komisji.

informacyjnego powodują niepewność wśród dzieci i ich rodziców w kontekście stosowania ich praw w zakresie ochrony danych na jednolitym rynku. Ta fragmentacja stwarza również wyzwania dla prowadzenia działalności transgranicznej oraz innowacji, w szczególności w odniesieniu do nowych rozwiązań technologicznych i rozwiązań z zakresu cyberbezpieczeństwa. Aby zapewnić skuteczne funkcjonowanie rynku wewnętrznego i uniknąć niepotrzebnych obciążeń dla przedsiębiorstw, istotne jest również, aby przepisy krajowe nie wykraczały poza marginesy określone w RODO ani nie wprowadzały dodatkowych wymogów w przypadku braku marginesu.

Szczególnym wyzwaniem w odniesieniu do przepisów krajowych jest uzgodnienie prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji oraz właściwe wyważenie tych praw. W niektórych przepisach krajowych ustanowiono zasadę pierwszeństwa wolności wypowiedzi, podczas gdy w innych pierwszeństwo ma ochrona danych osobowych, a przepisy o ochronie danych osobowych nie są stosowane wyłącznie w określonych sytuacjach, na przykład gdy chodzi o osobę o statusie osoby publicznej. Ponadto w innych państwach członkowskich prawodawca przewiduje pewne równoważenie praw lub ocenę poszczególnych przypadków w odniesieniu do odstępstw od niektórych przepisów RODO.

Komisja będzie nadal dokonywać oceny przepisów krajowych. Godzenie praw musi być przewidziane ustawą, szanować istotę praw podstawowych oraz być proporcjonalne i konieczne[40]. Przepisy dotyczące ochrony danych (jak również ich wykładnia i stosowanie) nie powinny mieć wpływu na korzystanie z prawa do wolności wypowiedzi i informacji, na przykład przez tworzenie efektu zniechęcającego lub wywieranie presji na dziennikarzy w celu ujawnienia ich źródeł. Wyważenie tych dwóch praw na mocy prawa krajowego powinno opierać się na orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka[41].

W przepisach państw członkowskich istnieją różne podejścia do wprowadzania odstępstw od ogólnego zakazu przetwarzania określonych kategorii danych osobowych, w odniesieniu do poziomu specyfikacji i zabezpieczeń, w tym do celów zdrowotnych i badawczych. W celu rozwiązania tej kwestii Komisja w pierwszej kolejności zidentyfikowała różne podejścia państw członkowskich[42] i w kolejnych krokach poprze ustanowienie kodeksów postępowania, które przyczyniłyby się do bardziej spójnego podejścia w tym obszarze oraz ułatwiły transgraniczne przetwarzanie danych osobowych.[43] Ponadto przyszłe wytyczne EROD w sprawie wykorzystywania danych osobowych w dziedzinie badań naukowych przyczynią się do zharmonizowanego podejścia. Komisja wniesie wkład do ustaleń EROD, w szczególności w odniesieniu do badań naukowych w dziedzinie zdrowia, w tym w formie konkretnych pytań i analizy scenariuszy, które otrzymała od środowiska naukowego.

---

[40] Art. 52 ust. 1 Karty.

[41] Zob. pkt 3.1 dokumentu roboczego służb Komisji: Godzenie prawa do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji.

[42] Komisja rozpoczęła badanie dotyczące oceny przepisów państw członkowskich w dziedzinie danych w zakresie zdrowia w świetle RODO", Chafea/2018/Health/03, umowa szczegółowa nr 2019 70 01.

[43] Zob. działania zapowiedziane w europejskiej strategii w zakresie danych, s. 30.

Wzmocnienie pozycji osób fizycznych w zakresie kontrolowania ich danych

Według badania dotyczącego praw podstawowych[44] 69 % ludności UE w wieku powyżej 16 lat słyszało o RODO, a 71 % osób w UE wie o istnieniu krajowego organu ochrony danych.

Osoby fizyczne są coraz bardziej świadome swoich praw: prawa w zakresie dostępu do swoich danych osobowych, ich poprawiania, usuwania i przenoszenia, prawo do sprzeciwu wobec ich przetwarzania, jak również do większej przejrzystości. W ramach RODO wzmocniono prawa procesowe obejmujące prawo do złożenia skargi do organu ochrony danych, w tym poprzez powództwa przedstawicielskie, oraz prawo do dochodzenia roszczeń na drodze sądowej. Osoby fizyczne coraz częściej korzystają z tych praw, ale istnieje również potrzeba ułatwienia ich wykonywania i pełnego egzekwowania. Dyskusje prowadzone przez EROD pozwolą na wyjaśnienie i dalsze ułatwienie korzystania z praw indywidualnych, podczas gdy proponowana dyrektywa w sprawie powództw przedstawicielskich[45], po jej przyjęciu, ma umożliwić poszczególnym osobom wnoszenie powództw zbiorowych we wszystkich państwach członkowskich i obniżyć koszty działań transgranicznych.

Prawo do przenoszenia danych ma wyraźny potencjał, wciąż nie w pełni wykorzystywany, do umiejscowienia osób fizycznych w centrum gospodarki opartej na danych, umożliwiając im zmianę usługodawców, łączenie różnych usług, korzystanie z innych innowacyjnych usług oraz wybór usług najbardziej przyjaznych w kontekście ochrony danych. Będzie to pośrednio sprzyjać konkurencji i wspierać innowacje. Uwolnienie tego potencjału jest jednym z priorytetów Komisji, w szczególności dlatego, że coraz częściej korzysta się z urządzeń związanych z internetem rzeczy, a konsumenci generują coraz więcej danych, przy czym mogą oni zetknąć się ze stosowaniem nieuczciwych praktyk i efektem uzależnienia od dostawcy. Możliwość przenoszenia może przynieść istotne korzyści w odniesieniu do zdrowia i dobrobytu, zmniejszyć ślad środowiskowy i dostęp do usług publicznych i prywatnych, zwiększyć wydajność produkcji oraz podnieść jakość i bezpieczeństwo produktów.

W ramach strategii w zakresie danych podkreślono potrzebę rozwiązania problemów takich jak brak norm umożliwiających udostępnianie danych w formacie nadającym się do odczytu maszynowego w celu zwiększenia możliwości rzeczywistego korzystania z prawa do przenoszenia danych, które jest obecnie ograniczone do kilku sektorów (np. bankowości i telekomunikacji). Można to osiągnąć przede wszystkim przez opracowanie odpowiednich narzędzi, znormalizowanego formatu i interfejsów[46]. Korzystanie w większym stopniu z tego prawa można by również osiągnąć dzięki wprowadzeniu interfejsów technicznych i formatów nadających się do odczytu maszynowego umożliwiających przenoszenie danych w czasie rzeczywistym. Zwiększone korzystanie z prawa do przenoszenia danych może między

[44] Agencja Praw Podstawowych Unii Europejskiej (FRA) (2020): ankieta dot. praw podstawowych z 2019 r. Ochrona danych i technologia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[45] Oczekuje się, że proponowana dyrektywa w sprawie powództw przedstawicielskich w celu ochrony zbiorowych interesów konsumentów (COM(2018) 184 final – 2018/089 (COD)), po jej przyjęciu, wzmocni ramy powództw przedstawicielskich również w dziedzinie ochrony danych.

[46] Może to obejmować m.in. narzędzia zarządzania zgodą oraz aplikacje zarządzania danymi osobowymi.

innymi ułatwić osobom fizycznym udostępnianie ich danych dla dobra publicznego (na przykład w celu wspierania badań w sektorze zdrowia), jeśli sobie tego życzą („altruistyczne podejście do danych"). W ramach przygotowywania pakietu dotyczącego usług cyfrowych[47] Komisja zbada szerzej rolę danych i praktyk związanych z danymi w ekosystemie platform.

[47] https://ec.europa.eu/commission/presscorner/detail/pl/ip_20_962

Możliwości i wyzwania dla organizacji, w szczególności dla małych i średnich przedsiębiorstw

RODO wraz z rozporządzeniem w sprawie ram swobodnego przepływu danych nieosobowych[48] oferuje przedsiębiorstwom możliwości w zakresie wspierania konkurencji i innowacji, zapewnienia swobodnego przepływu danych w UE oraz stworzenia równych warunków działania dla przedsiębiorstw mających siedzibę poza UE[49]. Prawo do przenoszenia danych, w połączeniu z rosnącą liczbą osób poszukujących rozwiązań bardziej sprzyjających ochronie prywatności, może zmniejszyć bariery wejścia na rynek dla przedsiębiorstw i otworzyć możliwości wzrostu w oparciu o zaufanie i innowacje. Niektóre zainteresowane strony informują, że stosowanie RODO stanowi wyzwanie zwłaszcza dla małych i średnich przedsiębiorstw (MŚP). Zgodnie z podejściem opartym na analizie ryzyka przyznawanie odstępstw na podstawie wielkości operatorów nie byłoby podejściem właściwym, ponieważ ich rozmiar sam w sobie nie stanowi wskaźnika ryzyka, jakie przetwarzanie danych osobowych, którego to przedsiębiorstwo się podejmuje, może stworzyć dla osób fizycznych. Kilka organów ochrony danych dostarczyło praktyczne narzędzia ułatwiających wdrożenie RODO przez MŚP prowadzące działalność w zakresie przetwarzania o niskim ryzyku. Wysiłki te powinny zostać zintensyfikowane i rozpowszechnione, najlepiej w ramach wspólnego europejskiego podejścia, aby nie tworzyć barier dla jednolitego rynku.

Organy ochrony danych opracowały szereg działań mających pomóc MŚP w przestrzeganiu przepisów ogólnego rozporządzenia o ochronie danych, na przykład przez udostępnienie szablonów i zapisów dotyczących czynności przetwarzania, a także seminariów i gorących linii przeznaczonych do konsultacji. Wiele z tych inicjatyw skorzystało z finansowania UE[50]. Należy rozważyć dalsze działania mające na celu ułatwienie stosowania RODO w odniesieniu do MŚP.

RODO udostępnia zestaw narzędzi wszystkim rodzajom przedsiębiorstw i organizacji, aby pomóc im w wykazaniu zgodności, takich jak kodeksy postępowania, mechanizmy certyfikacji i standardowe klauzule umowne. Należy w pełni wykorzystywać ten zestaw narzędzi. MŚP podkreślają w szczególności znaczenie i użyteczność kodeksów postępowania dostosowanych do ich sytuacji i niepowodujących niewspółmiernych kosztów. W odniesieniu do systemów certyfikacji bezpieczeństwo (w tym cyberbezpieczeństwo) i ochrona danych w fazie projektowania są kluczowymi elementami, które należy uwzględnić w RODO i które skorzystałyby na wspólnym i ambitnym podejściu w całej UE. Komisja pracuje

[48] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, Dz.U. L 303 z 28.11.2018, s. 59.

[49] Zob. pkt 5 dokumentu roboczego służb Komisji. Zob. również COM(2019) 250 final, Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, wyjaśniające zasady regulujące przetwarzanie mieszanych zbiorów danych, składających się zarówno z danych osobowych, jak i nieosobowych, i zawierające praktyczne rozwiązania dla przedsiębiorstw, w tym dla MŚP.

[50] Komisja udzieliła wsparcia finansowego w postaci trzech fal dotacji, na łączną kwotę 5 mln EUR, przy czym dwie ostatnie są przeznaczone specjalnie na wspieranie krajowych organów ochrony danych w wysiłkach na rzecz dotarcia do osób fizycznych oraz małych i średnich przedsiębiorstw: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_pl. Dodatkowa kwota w wysokości 1 mln EUR zostanie przydzielona w 2020 r.

obecnie nad standardowymi klauzulami umownymi między administratorami a podmiotami przetwarzającymi[51], opierając się na trwających pracach nad modernizacją standardowych klauzul umownych dotyczących przekazywania za granicę[52].

Stosowanie RODO w kontekście nowych technologii

Jako opracowane w sposób neutralny pod względem technicznym RODO opiera się na zasadach i w związku z tym jest może uwzględniać nowe technologie w miarę ich rozwoju.

Rozporządzenie jest postrzegane jako niezbędne i elastyczne narzędzie gwarantujące, że rozwój nowych technologii jest zgodny z prawami podstawowymi. Ramy prawne dotyczące ochrony danych i prywatności dowiodły swej wagi i elastyczności podczas kryzysu związanego z emisją COVID-19, w szczególności w odniesieniu do projektowania aplikacji do śledzenia kontaktów i innych rozwiązań technologicznych mających na celu zwalczanie pandemii. Przyszłe wyzwania wiążą się z potrzebą wyjaśnienia sposobu stosowania sprawdzonych zasad do konkretnych technologii, takich jak sztuczna inteligencja, łańcuch bloków, internet rzeczy lub rozpoznawanie twarzy, które wymagają ciągłego monitorowania. Na przykład biała księga Komisji w sprawie sztucznej inteligencji[53] otworzyła debatę publiczną na temat konkretnych okoliczności, które mogłyby uzasadniać wykorzystanie sztucznej inteligencji do celów zdalnej identyfikacji biometrycznej (np. rozpoznawania twarzy) w miejscach publicznych, oraz na temat ogólnych zabezpieczeń. W związku z tym organy ochrony danych powinny być zawczasu gotowe do udziału w projektowaniu technicznym.

Ponadto zasadniczym elementem ochrony osób fizycznych jest zdecydowane i skuteczne egzekwowanie RODO w odniesieniu do dużych platform cyfrowych i zintegrowanych przedsiębiorstw, w tym w takich obszarach jak reklama internetowa i mikrotargetowanie.

Opracowanie nowoczesnego międzynarodowego zestawu narzędzi do przekazywania danych

W ramach RODO przewidziano unowocześniony zestaw narzędzi ułatwiających przekazywanie danych osobowych z UE do państw trzecich lub organizacji międzynarodowych, przy jednoczesnym zapewnieniu dalszego korzystania z wysokiego poziomu ochrony danych. W ciągu ostatnich dwóch lat Komisja zintensyfikowała prace mające na celu wykorzystanie pełnego potencjału narzędzi dostępnych w ramach RODO.

Prace te polegały m.in. na aktywnej współpracy z kluczowymi partnerami w celu wydania „decyzji stwierdzającej odpowiedni stopień ochrony. Wskutek takiej decyzji możliwy staje się bezpieczny swobodny przepływ danych osobowych do danego państwa trzeciego bez potrzeby przedstawiania dodatkowych gwarancji przez podmiot przekazujący dane lub uzyskania przez niego odpowiedniego upoważnienia. W szczególności wzajemne decyzje stwierdzające odpowiedni stopień ochrony

[51] Zgodnie z art. 28 RODO.
[52] Zgodnie z art. 46 RODO.
[53] Biała księga w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania – COM(2020) 65 final.

przyjęte przez UE i Japonię, które weszły w życie w lutym 2019 r., stworzyły największy na świecie obszar wolnych i bezpiecznych przepływów danych. Ponadto proces związany z decyzjami stwierdzającymi odpowiedni stopień ochrony w stosunku do Republiki Korei jest na zaawansowanym etapie i prowadzone są rozmowy wstępne z innymi ważnymi partnerami w Azji i Ameryce Łacińskiej.

Stwierdzenie odpowiedniego stopnia ochrony odgrywa również ważną rolę w kontekście przyszłych stosunków ze Zjednoczonym Królestwem, pod warunkiem że spełnione są odpowiednie warunki. Stanowi on czynnik wspomagający handel, w tym cyfrowy, i jest niezbędnym warunkiem ścisłej i ambitnej współpracy w dziedzinie egzekwowania prawa i bezpieczeństwa. Ponadto wysoki stopień konwergencji w zakresie ochrony danych jest ważnym elementem zapewnienia równych warunków działania między dwiema tak ściśle zintegrowanymi gospodarkami. Zgodnie z deklaracją polityczną w sprawie przyszłych stosunków między UE a Zjednoczonym Królestwem Komisja prowadzi obecnie ocenę stopnia ochrony na podstawie zarówno RODO, jak i dyrektywy o ochronie danych w sprawach karnych[54].

W ramach pierwszej oceny RODO Komisja jest również zobowiązana do dokonania przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które zostały przyjęte na mocy poprzednich przepisów[55]. Służby Komisji zaangażowały się w intensywny dialog z każdym z 11 zainteresowanych państw trzecich i terytoriów[56] w celu dokonania oceny rozwoju ich systemów ochrony danych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony oraz tego, czy spełniają one standardy określone w RODO. Potrzeba zapewnienia ciągłości takich decyzji – kluczowego narzędzia handlu i współpracy międzynarodowej – jest jednym z czynników, które skłoniły kilka z tych państw i terytoriów do modernizacji i wzmocnienia ich prawa w zakresie ochrony prywatności. Z niektórymi z tych państw i terytoriów omawiane są dodatkowe zabezpieczenia w celu wyeliminowania istotnych różnic w zakresie ochrony. Biorąc jednak pod uwagę fakt, że Trybunał Sprawiedliwości w wyroku, który ma zostać wydany w dniu 16 lipca, może przedstawić wyjaśnienia, które mogą mieć znaczenie dla niektórych elementów normy dotyczącej odpowiedniego stopnia ochrony, Komisja przedstawi oddzielnie sprawozdanie na temat oceny istniejących orzeczeń w sprawie odpowiedniej ochrony danych osobowych po wydaniu przez Trybunał Sprawiedliwości wyroku w tej sprawie[57].

---

[54] 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, s. 89.

[55] 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, Dz.U. L 281 z 23.11.1995, s. 31.

[56] Te państwa i terytoria to: Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Jersey, Wyspa Man, Izrael, Nowa Zelandia, Szwajcaria i Urugwaj.

[57] Zob. sprawa C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Limited, Maximillian Schrems („Schrems II”), która dotyczy orzeczenia w trybie prejudycjalnym dotyczącego tzw. standardowych klauzul umownych. Trybunał może jednak również doprecyzować niektóre elementy normy dotyczącej odpowiedniego stopnia ochrony.

Oprócz prac w zakresie odpowiedniego stopnia ochrony Komisja pracuje nad kompleksową modernizacją standardowych klauzul umownych w celu ich zaktualizowania w świetle nowych wymogów wprowadzonych na mocy RODO. Celem tych prac jest lepsze odzwierciedlenie realiów operacji przetwarzania w nowoczesnej gospodarce cyfrowej i rozważenie ewentualnej potrzeby dalszego sprecyzowania pewnych zabezpieczeń, w tym z uwzględnieniem przyszłego orzecznictwa Trybunału Sprawiedliwości[58]. Klauzule te stanowią zdecydowanie najbardziej rozpowszechnioną metodę przekazywania danych, co znajduje odzwierciedlenie w fakcie, że tysiące przedsiębiorstw unijnych bazuje na nich w celu świadczenia szerokiego zakresu usług na rzecz swoich klientów, dostawców, partnerów i pracowników.

EROD odegrał również aktywną rolę w opracowywaniu międzynarodowych aspektów RODO, która obejmowała m.in. aktualizację wytycznych dotyczących istniejących mechanizmów przekazywania danych, takich jak wiążące reguły korporacyjne i tzw. „odstępstwa", a także rozwój infrastruktury prawnej na potrzeby stosowania nowych narzędzi wprowadzonych na mocy RODO, tj. kodeksów postępowania i certyfikacji.

Aby umożliwić zainteresowanym stronom pełne korzystanie z zestawu narzędzi RODO, ważne jest, aby EROD zintensyfikował prace nad różnymi mechanizmami przekazywania danych, w tym przez dalsze usprawnianie procesu zatwierdzania wiążących reguł korporacyjnych, sfinalizowanie wytycznych dotyczących kodeksów postępowania i certyfikacji jako narzędzi przekazywania danych oraz wyjaśnienie powiązań między przepisami dotyczącymi przekazywania danych za granicę (rozdział V) a terytorialnym zakresem stosowania RODO (art. 3).

Innym ważnym aspektem międzynarodowego wymiaru przepisów UE dotyczących ochrony danych jest rozszerzony zakres terytorialny ogólnego rozporządzenia o ochronie danych, który obejmuje również działania podmiotów zagranicznych prowadzących działalność w zakresie przetwarzania danych na rynku UE. Odpowiednie uwzględnienie tego rozszerzenia w działaniach organów ochrony danych dotyczących egzekwowania prawa ma zasadnicze znaczenie dla zapewnienia faktycznego przestrzegania RODO i prawdziwie równych warunków działania. Organy te powinny w szczególności nawiązać współpracę, w razie konieczności, z przedstawicielem administratora danych lub podmiotu przetwarzającego w UE, do którego można zwracać się w uzupełnieniu lub zamiast do przedsiębiorstwa mającego siedzibę poza UE. Podejście to powinno być energicznie realizowane w celu wysłania wyraźnej wiadomości, że brak siedziby w UE nie zwalnia zagranicznych podmiotów z obowiązków wynikających z RODO.

Wspieranie konwergencji i międzynarodowej współpracy w dziedzinie ochrony danych

RODO stało się już kluczowym punktem odniesienia na szczeblu międzynarodowym i stanowiło katalizator dla wielu krajów na świecie, aby rozważyć wprowadzenie nowoczesnych przepisów dotyczących prywatności. Ta tendencja w kierunku globalnej konwergencji jest bardzo pozytywnym zjawiskiem, które stwarza nowe

[58] Zob. sprawa Schrems II.

możliwości lepszej ochrony osób fizycznych w UE, gdy ich dane są przekazywane za granicę, a jednocześnie ułatwia przepływ danych.

W oparciu o tę tendencję Komisja zintensyfikowała dialog na wielu forach dwustronnych, regionalnych i wielostronnych, aby wspierać globalną kulturę poszanowania prywatności i opracować elementy konwergencji między różnymi systemami ochrony prywatności. W swoich wysiłkach Komisja powołała się na aktywne wsparcie Europejskiej Służby Działań Zewnętrznych i sieci delegatur UE w państwach trzecich oraz misji przy organizacjach międzynarodowych i zamierza również powoływać się na nie w przyszłości. Pozwoliło to również osiągnąć większą spójność i komplementarność różnych aspektów zewnętrznego wymiaru polityki UE – od handlu do nowego partnerstwa między UE a Afryką. Grupa G20 i grupa G7 również doceniły niedawno wkład ochrony danych w zaufanie do gospodarki cyfrowej i przepływów danych, w szczególności poprzez koncepcję „Data Free Flow with Trust" (ang. „swobodny przepływ danych oparty na zaufaniu"), którą pierwotnie zaproponowała japońska prezydencja G20.[59] Strategia w zakresie danych podkreśla, że Komisja zamierza nadal promować wymianę danych z zaufanymi partnerami, a jednocześnie zwalczać nadużycia, takie jak nieproporcjonalny dostęp (zagranicznych) organów publicznych do danych osobowych.

Propagując konwergencję standardów ochrony danych na szczeblu międzynarodowym, jako sposób na ułatwienie przepływu danych, a co za tym idzie, na wymianę handlową, Komisja jest również zdecydowana przeciwdziałać protekcjonizmowi cyfrowemu, co zostało niedawno podkreślone w ramach strategii w zakresie danych.[60] W tym celu opracowała szczegółowe przepisy dotyczące przepływu danych i ochrony danych w umowach handlowych[61], które systematycznie uwzględnia w umowach dwustronnych – ostatnio z Australią, Nową Zelandią i Zjednoczonym Królestwem – oraz negocjacjach wielostronnych, takich jak obecne rozmowy w ramach WTO w sprawie handlu elektronicznego[62]. Te przepisy horyzontalne wykluczają nieuzasadnione ograniczenia, takie jak przymusowe wymogi dotyczące lokalizacji danych, a z drugiej strony zachowują autonomię regulacyjną stron w zakresie ochrony podstawowego prawa do ochrony danych.

Należy zatem dalej badać możliwości synergii między instrumentami ochrony handlu i danych w celu zapewnienia swobodnego i bezpiecznego międzynarodowego przepływu danych, który ma zasadnicze znaczenie dla działalności gospodarczej, konkurencyjności i rozwoju europejskich przedsiębiorstw, w tym MŚP, w coraz bardziej cyfrowej gospodarce.

---

[59] Zob. np. treść deklaracji przywódców grupy G20: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Strategia w zakresie danych, s. 23.

[61] Zob. tekst przepisów horyzontalnych dotyczących transgranicznych przepływów danych i ochrony danych osobowych (w unijnych umowach handlowych i inwestycyjnych): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] 84 członków WTO jest obecnie zaangażowanych w wielostronne negocjacje w sprawie handlu elektronicznego w związku ze wspólną deklaracją przyjętą przez ministrów w dniu 25 stycznia 2019 r. w Davos. W ramach tego procesu UE przedłożyła 3 maja 2019 r. tekst wniosku w sprawie przyszłych przepisów i obowiązków w zakresie handlu elektronicznego. Wniosek zawiera przepisy horyzontalne dotyczące przepływu danych i ochrony danych osobowych: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

Podobnie ważne jest zagwarantowanie, aby w przypadku gdy przedsiębiorstwa działające na rynku europejskim zostaną wezwane na podstawie uzasadnionego wniosku o udostępnienie danych do celów egzekwowania prawa, mogły tego dokonać bez ryzyka kolizji przepisów i przy pełnym poszanowaniu praw podstawowych UE. Aby usprawnić takie przekazywanie danych, Komisja zobowiązuje się do opracowania odpowiednich ram prawnych z partnerami międzynarodowymi w celu unikania kolizji przepisów i wspierania efektywnych form współpracy, zwłaszcza przez zapewnienie niezbędnych zabezpieczeń w zakresie ochrony danych, a tym samym przyczynienia się do skuteczniejszej walki z przestępczością.

Ponadto w sytuacjach, w których kwestie związane z przestrzeganiem prawa do prywatności lub incydenty związane z bezpieczeństwem danych mogą mieć wpływ na dużą liczbę osób w kilku jurysdykcjach jednocześnie, należy jeszcze bardziej zacieśnić współpracę w terenie między europejskimi i międzynarodowymi organami regulacyjnymi. Wymaga to w szczególności opracowania odpowiednich instrumentów prawnych w celu zacieśnienia współpracy i wzajemnej pomocy, w tym przez umożliwienie niezbędnej wymiany informacji w kontekście dochodzeń. W tym właśnie duchu Komisja powołuje Akademię Ochrony Danych (Data Protection Academy), platformę, w ramach której unijne i zagraniczne organy ochrony danych dzielą się wiedzą, doświadczeniem i najlepszymi praktykami w celu ułatwienia i wspierania współpracy między organami odpowiedzialnymi za egzekwowanie prawa w zakresie ochrony prywatności.

3 DALSZE DZIAŁANIA

Aby w pełni zrealizować potencjał RODO, ważne jest stworzenie zharmonizowanego podejścia i wspólnej europejskiej kultury ochrony danych oraz wspieranie bardziej skutecznego i zharmonizowanego postępowania w sprawach transgranicznych. Jest to zgodne z oczekiwaniami ludzi i przedsiębiorstw oraz stanowi zasadniczy cel reformy unijnych przepisów o ochronie danych. Równie ważne jest zagwarantowanie, aby wszystkie narzędzia dostępne w RODO były w pełni wykorzystywane w celu zapewnienia skutecznego stosowania tego rozporządzenia w odniesieniu do osób fizycznych i przedsiębiorstw.

Komisja będzie kontynuować dwustronną wymianę informacji z państwami członkowskimi na temat wdrażania RODO i, w razie potrzeby, będzie nadal wykorzystywać wszystkie dostępne narzędzia do zapewnienia przestrzegania przez państwa członkowskie zobowiązań wynikających z RODO.

Biorąc pod uwagę ciągłą ocenę przepisów krajowych, krótki okres praktycznego stosowania przepisów RODO oraz fakt, że w wielu państwach członkowskich prawodawstwo sektorowe jest wciąż poddawane przeglądowi, wyciąganie ostatecznych wniosków na temat obecnego poziomu fragmentacji byłoby przedwczesne. W kontekście ewentualnej kolizji przepisów w związku z wdrożeniem przez państwa członkowskie klauzul precyzujących należy najpierw lepiej zrozumieć konsekwencje dla administratorów danych i podmiotów przetwarzających[63].

[63] Zob. stanowisko Rady i ustalenia w sprawie stosowania RODO.

Podejmując działania następcze w związku z tymi kwestiami, można odwoływać się do stosownego orzecznictwa sądów krajowych i Trybunału Sprawiedliwości, które przyczynia się do stworzenia spójnej wykładni przepisów o ochronie danych. Sądy krajowe wydały ostatnio wyroki w sprawie unieważnienia przepisów prawa krajowego, które odbiegają od przepisów RODO[64].

W wymiarze międzynarodowym Komisja będzie nadal koncentrować się na wspieraniu konwergencji przepisów o ochronie danych w celu zapewnienia bezpiecznego przepływu danych. Dotyczy to różnych form pracy proaktywnej, na przykład w kontekście trwających reform w zakresie nowych lub zaktualizowanych przepisów o ochronie danych lub dążenia do koncepcji „swobodnego przepływu danych opartego na zaufaniu" na forach wielostronnych. Powyższe działania obejmują również różne dialogi dotyczące odpowiedniego stopnia ochrony oraz modernizację i rozbudowę naszego zestawu narzędzi do przekazywania danych przez aktualizację standardowych klauzul umownych i stworzenie podstaw mechanizmów certyfikacji. Prace te obejmują również negocjacje międzynarodowe, np. w dziedzinie transgranicznego dostępu do dowodów elektronicznych, w celu zagwarantowania, by przekazywanie danych odbywało się przy zastosowaniu odpowiednich zabezpieczeń w zakresie ochrony danych. Wreszcie, angażując się w negocjacje w sprawie współpracy międzynarodowej i wzajemnej pomocy między organami odpowiedzialnymi za egzekwowanie przepisów w zakresie ochrony danych, Komisja będzie dążyć do konwergencji przepisów w tym obszarze.

Na podstawie tej oceny stosowania RODO od maja 2018 r. wymienione poniżej działania zostały uznane za konieczne do wspierania jego stosowania. Komisja będzie monitorować ich wdrażanie również w kontekście zbliżającego się sprawozdania z oceny w 2024 r.

Wdrażanie i uzupełnianie ram prawnych

Państwa członkowskie powinny:

- zakończyć proces dostosowywania własnych przepisów sektorowych do przepisów RODO;
- rozważyć ograniczenie stosowania klauzul precyzujących, które mogłyby prowadzić do fragmentacji i zagrozić swobodnemu przepływowi danych w UE;
- ocenić, czy krajowe przepisy wdrażające RODO przewidują wszystkie okoliczności w ramach marginesu przewidzianego dla przepisów państwa członkowskiego.

Komisja będzie:

- prowadzić dwustronną wymianę z państwami członkowskimi na temat zgodności przepisów krajowych z RODO, w tym na temat niezależności i zasobów krajowych organów ochrony danych; wykorzystywać wszystkie dostępne narzędzia, w tym postępowania w sprawie uchybienia

[64] Tak było w przypadku Niemiec, Hiszpanii i Austrii, a wyroki te pozwoliły wypełnić luki w przepisach krajowych.

zobowiązaniom państwa członkowskiego, w celu zagwarantowania, by państwa członkowskie przestrzegały RODO;

- wspierać dalszą wymianę poglądów i praktyk krajowych między państwami członkowskimi na tematy, które podlegają dalszemu doprecyzowaniu na szczeblu krajowym, w celu zredukowania stopnia fragmentacji jednolitego rynku, takie jak przetwarzanie danych osobowych związane ze zdrowiem i badaniami, lub które należy równoważyć z innymi prawami, takimi jak wolność wypowiedzi;
- zapewniać spójne stosowanie ram ochrony danych w odniesieniu do nowych technologii w celu wspierania innowacji i rozwoju technologicznego;
- wykorzystywać wysiłki grupy ekspertów ds. RODO z państw członkowskich (ustanowionej na etapie przejściowym przed wejściem rozporządzenia w życie) w celu ułatwienia dyskusji i wymiany doświadczeń między państwami członkowskimi i z Komisją;
- badać, czy – w świetle dalszych doświadczeń i stosownego orzecznictwa – zaproponowanie ewentualnych przyszłych ukierunkowanych zmian w niektórych przepisach RODO może być właściwe, w szczególności w odniesieniu do dokumentacji dotyczącej przetwarzania danych przez MŚP, które nie przetwarzają danych osobowych w ramach podstawowej działalności (niskie ryzyko)[65], oraz ewentualnej harmonizacji wieku wyrażenia zgody przez dzieci w zakresie świadczenia usług społeczeństwa informacyjnego.

Pełne wykorzystanie potencjału nowego systemu zarządzania

EROD oraz organy ochrony danych wzywa się do:

- opracowania skutecznych rozwiązań między organami ochrony danych dotyczących funkcjonowania mechanizmu współpracy i spójności, w tym aspektów proceduralnych, w oparciu o wiedzę fachową ich członków oraz przez zwiększenie zaangażowania sekretariatu;
- wspierania harmonizacji stosowania i egzekwowania przepisów RODO przy użyciu wszelkich dostępnych środków, w tym przez dalsze doprecyzowanie kluczowych pojęć RODO, oraz zagwarantowanie, by krajowe wytyczne były w pełni zgodne z wytycznymi przyjętymi przez EROD;
- zachęcania do stosowania wszystkich narzędzi przewidzianych w przepisach RODO w celu zapewnienia ich spójnego stosowania;
- zacieśniania współpracy między organami ochrony danych, na przykład przez prowadzenie wspólnych dochodzeń.

Komisja będzie:

- nadal ściśle monitorować efektywną i pełną niezależność krajowych organów ochrony danych;

[65] Art. 30 ust. 5 RODO.

- zachęcać do współpracy między organami regulacyjnymi (w szczególności w takich obszarach jak konkurencja, łączność elektroniczna, bezpieczeństwo sieci i systemów informatycznych oraz polityka konsumencka);
- sprzyjać podejmowaniu odpowiednich działań przez EROD w kontekście procedur stosowanych przez krajowe organy ochrony danych w celu poprawy współpracy w sprawach transgranicznych.

Państwa członkowskie powinny

- przydzielać zasoby organom ochrony danych wystarczające do wykonywania ich zadań.

Wspieranie zainteresowanych stron

EROD oraz organy ochrony danych wzywa się do:

- przyjmowania dalszych praktycznych, łatwych do zrozumienia wytycznych, które dostarczają jasnych odpowiedzi i pozwalają uniknąć niejednoznaczności w kwestiach związanych ze stosowaniem RODO, na przykład w odniesieniu do przetwarzania danych dzieci i osób, których dane dotyczą, w tym do korzystania z prawa do dostępu i prawa do usunięcia danych, z zainteresowanymi stronami uczestniczącymi w tym procesie;
- dokonywania przeglądu wytycznych w przypadku, gdy konieczne są dalsze wyjaśnienia w świetle doświadczeń i zmian, w tym w orzecznictwie Trybunału Sprawiedliwości;
- opracowania praktycznych narzędzi, takich jak zharmonizowane formularze na potrzeby naruszeń ochrony danych oraz uproszczone rejestry działań związanych z przetwarzaniem, aby pomóc małym i średnim przedsiębiorstwom o niskim poziomie ryzyka w wypełnianiu ich obowiązków.

Komisja będzie:

- zapewniać standardowe klauzule umowne zarówno w odniesieniu do przekazywania danych za granicę, jak i relacji między administratorem danych a podmiotem przetwarzającym;
- zapewniać narzędzia wyjaśniające/wspierające stosowanie przepisów o ochronie danych w odniesieniu do dzieci[66];
- zgodnie ze strategią w zakresie danych, badać praktyczne środki ułatwiające szerszy zakres korzystania z prawa do przenoszenia danych przez osoby fizyczne, takie jak zapewnienie im większej kontroli nad tym, kto może uzyskać dostęp do maszynowo generowanych danych i je wykorzystywać;
- wspierać standaryzację/certyfikację, w szczególności w odniesieniu do aspektów cyberbezpieczeństwa, poprzez współpracę między Agencją Unii

[66] Projekt Komisji w sprawie narzędzi identyfikacji wieku – projekt pilotażowy w celu zademonstrowania interoperacyjnej infrastruktury technicznej w zakresie ochrony dzieci, w tym weryfikacji wieku i zgody rodziców. Oczekuje się, że przyczyni się to do wdrożenia mechanizmów ochrony dzieci w oparciu o istniejące przepisy UE dotyczące ochrony dzieci w internecie.

Europejskiej ds. Cyberbezpieczeństwa (ENISA), organami ochrony danych i EROD;

- w stosownych przypadkach, korzystać z prawa do zwrócenia się do EROD o przygotowanie wytycznych i opinii na temat konkretnych kwestii istotnych dla zainteresowanych stron;
- w razie potrzeby, określać wytyczne, przy pełnym poszanowaniu roli EROD;
- wspierać działania organów ochrony danych, które ułatwiają MŚP wypełnianie obowiązków wynikających z RODO, poprzez wsparcie finansowe, w szczególności w zakresie praktycznych wytycznych i narzędzi cyfrowych, które mogą być powielane w innych państwach członkowskich.

Zachęcanie do nowatorstwa

Komisja będzie:

- monitorować stosowanie przepisów RODO w odniesieniu do nowych technologii, uwzględniając również ewentualne przyszłe inicjatywy w obszarze sztucznej inteligencji i w ramach strategii w zakresie danych;
- zachęcać, w tym poprzez wsparcie finansowe, do opracowywania unijnych kodeksów postępowania w dziedzinie zdrowia i badań naukowych;
- uważnie śledzić rozwój i stosowanie aplikacji w kontekście pandemii COVID-19.

EROD wzywa się do:

- wydawania wytycznych w sprawie stosowania RODO w obszarze badań naukowych, sztucznej inteligencji, łańcucha bloków i ewentualnych innych rozwiązań technologicznych;
- dokonywania przeglądu wytycznych, w przypadku gdy konieczne są dalsze wyjaśnienia w kontekście rozwoju technologicznego.

Dalszy rozwój zestawu narzędzi służących do przekazywania danych

Komisja będzie:

- prowadzić dialog na temat odpowiedniej ochrony danych osobowych z zainteresowanymi państwami trzecimi, zgodnie ze strategią określoną w komunikacie z 2017 r. pt. „Wymiana i ochrona danych osobowych w zglobalizowanym świecie”, w tym, w miarę możliwości, uwzględniając przekazywanie danych organom ścigania (na mocy dyrektywy o ochronie danych w sprawach karnych) i innym organom publicznym; obejmuje to również finalizację procesu stwierdzenie odpowiedniego stopnia ochrony w odniesieniu do Republiki Korei tak szybko, jak to możliwe;
- odpowiedzialna za finalizację trwającej oceny istniejących decyzji stwierdzających odpowiedni stopień ochrony danych osobowych i złożenie sprawozdań Parlamentowi Europejskiemu i Radzie;
- odpowiedzialna za finalizację prac nad modernizacją standardowych klauzul umownych – w celu ich aktualizacji w świetle ogólnego rozporządzenia

o ochronie danych – obejmujących wszystkie istotne scenariusze przekazywania i lepiej odzwierciedlających nowoczesne praktyki biznesowe.

EROD wzywa się do:

- dalszego doprecyzowania powiązań między przepisami dotyczącymi przekazywania danych za granicę (rozdział V) a terytorialnym zakresem stosowania RODO (art. 3);
- zapewnienia skutecznego egzekwowania przepisów w odniesieniu do podmiotów mających siedzibę w państwach trzecich objętych zakresem terytorialnym RODO, w tym w odniesieniu do wyznaczenia przedstawiciela, w stosownych przypadkach (art. 27);
- usprawnienia oceny i ostatecznego zatwierdzenia wiążących reguł korporacyjnych w celu przyspieszenia procesu;
- zakończenia prac nad strukturą, procedurami i kryteriami oceny w odniesieniu do kodeksów postępowania i mechanizmów certyfikacji jako narzędzi przekazywania danych.

Promowanie konwergencji i rozwijanie współpracy międzynarodowej

Komisja będzie:

- wspierać trwające procesy reform w państwach trzecich w zakresie nowych lub zmodernizowanych przepisów o ochronie danych przez dzielenie się doświadczeniami i najlepszymi praktykami;
- współpracować z partnerami z Afryki w celu promowania konwergencji regulacyjnej i wspierania budowania zdolności organów nadzorczych w ramach rozdziału cyfrowego nowego partnerstwa między UE a Afryką;
- prowadzić ocenę możliwości ułatwienia współpracy między podmiotami prywatnymi a organami ścigania, w tym przez negocjowanie dwustronnych i wielostronnych ram przekazywania danych w kontekście dostępu zagranicznych organów ścigania do dowodów elektronicznych, aby uniknąć kolizji przepisów przy jednoczesnym zapewnieniu odpowiednich zabezpieczeń w zakresie ochrony danych;
- współpracować z organizacjami międzynarodowymi i regionalnymi, takimi jak OECD, ASEAN lub grupa G-20, w celu wspierania zaufanych przepływów danych w oparciu o wysokie standardy ochrony danych, w tym w kontekście inicjatywy „Data Free Flow with Trust”;
- odpowiedzialna za utworzenie Akademii Ochrony Danych w celu ułatwienia i wspierania przekazywania danych między europejskimi i międzynarodowymi organami regulacyjnymi;
- wspierać międzynarodową współpracę w zakresie egzekwowania prawa między organami nadzoru, w tym przez negocjowanie umów o współpracy i wzajemnej pomocy.