KOMISJA
EUROPEJSKA

Bruksela, dnia 24.1.2018r.
COM(2018) 43 final

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.

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.

Wprowadzenie

W dniu 6 kwietnia 2016 r. UE wyraziła zgodę na przeprowadzenie ważnej reformy swoich ram ochrony danych, polegającej na przyjęciu pakietu dotyczącego reformy ochrony danych, w którego skład wchodzi ogólne rozporządzenie o ochronie danych (RODO)[1], zastępujące obowiązującą od dwudziestu lat dyrektywę 95/46/WE[2] („dyrektywa o ochronie danych"), i dyrektywa w sprawie policji[3]. Dnia 25 maja 2018 r., dwa lata po przyjęciu i wejściu w życie, rozpocznie się bezpośrednie stosowanie nowego, obejmującego swoim zasięgiem całą UE instrumentu ochrony danych – ogólnego rozporządzenia o ochronie danych („rozporządzenie")[4].

Nowe rozporządzenie wzmocni ochronę prawa osób fizycznych do ochrony danych osobowych, odzwierciedlając fakt, że ochrona danych stanowi prawo podstawowe Unii Europejskiej[5].

Zapewniając jeden zestaw przepisów mających bezpośrednie zastosowanie w porządku prawnym państw członkowskich, rozporządzenie zagwarantuje swobodny przepływ danych osobowych między państwami członkowskimi UE oraz wzmocni dwa nieodzowne elementy jednolitego rynku cyfrowego: zaufanie konsumentów i ich bezpieczeństwo. W ten sposób rozporządzenie wprowadzi nowe możliwości dla firm i przedsiębiorstw, szczególnie tych mniejszych, również za sprawą wyjaśnienia przepisów dotyczących międzynarodowego przekazywania danych.

Nowe ramy ochrony danych bazują wprawdzie na obowiązujących obecnie przepisach prawa, ich wprowadzenie będzie miało jednak daleko idące skutki i będzie wymagało znacznych dostosowań w określonych kwestiach. Z tego względu w rozporządzeniu przewidziano dwuletni okres przejściowy trwający do dnia 25 maja 2018 r., aby państwa członkowskie i zainteresowane strony miały czas w pełni przygotować się do stosowania nowych ram prawnych.

---

[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.

[2] 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.

[3] 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.

[4] Rozporządzenie weszło w życie w dniu 24 maja 2016 r. i będzie miało zastosowanie od dnia 25 maja 2018 r.

[5] Prawo to zapisano w art. 8 Karty praw podstawowych Unii Europejskiej i w art. 16 TFUE.

Przez ostatnie dwa lata wszystkie zainteresowane strony, od administracji krajowych i krajowych organów ochrony danych, aż po administratorów i podmioty przetwarzające, uczestniczyły w licznych działaniach, zapewniając, aby znaczenie i skala zmian wiążących się z nowymi przepisami o ochronie danych zostały dobrze zrozumiane, a wszystkie podmioty były gotowe do stosowania tych przepisów. W związku z tym, że do dnia 25 maja pozostało już mało czasu, Komisja jest zdania, że należy ocenić przeprowadzone prace i rozważyć wszelkie kolejne działania, które warto przeprowadzić w celu zapewnienia, aby wprowadzone zostały wszystkie elementy konieczne do skutecznego wejścia w życie nowych ram[6].

W niniejszym komunikacie:

- podsumowano najważniejsze innowacje i możliwości stwarzane przez nowe przepisy UE w dziedzinie ochrony danych;
- podsumowano prace przygotowawcze przeprowadzone dotychczas na szczeblu UE;
- przedstawiono dalsze działania, które powinny zostać podjęte przez Komisję Europejską, krajowe organy ochrony danych i krajowe administracje dla skutecznego zakończenia etapu przygotowań;
- określono środki, które Komisja zamierza podjąć w nadchodzących miesiącach.

Ponadto równolegle z przyjęciem niniejszego komunikatu Komisja uruchamia zestaw narzędzi internetowych, aby pomóc zainteresowanym stronom w przygotowaniach do stosowania rozporządzenia, oraz kampanię informacyjną we wszystkich państwach członkowskich, wspieraną przez biura przedstawicielstw.

1. NOWE UNIJNE RAMY OCHRONY DANYCH – WZMOCNIONA OCHRONA I NOWE MOŻLIWOŚCI

Rozporządzenie nadal bazuje wprawdzie na podejściu przyjętym w dyrektywie o ochronie danych, jednak wyjaśniono w nim i zaktualizowano przepisy o ochronie danych w oparciu o 20 lat doświadczeń w zakresie stosowania przepisów UE w dziedzinie ochrony danych i odpowiednie orzecznictwo z tego samego okresu; wprowadzono w nim szereg nowych elementów, które mają na celu wzmocnienie ochrony prawa osób fizycznych i stworzenie nowych możliwości dla firm i przedsiębiorstw. Należą do nich w szczególności:

- **zharmonizowane ramy prawne prowadzące do jednolitego stosowania przepisów z korzyścią dla unijnego jednolitego rynku cyfrowego.** Oznacza to jeden zestaw przepisów dla obywateli i przedsiębiorstw. Jest to odpowiedź na panującą obecnie sytuację, w której państwa członkowskie UE wykonują przepisy dyrektywy w różny sposób. Aby zapewnić jednakowe i spójne stosowanie przepisów we wszystkich państwach członkowskich, wprowadza się mechanizm kompleksowej współpracy;

- **równe warunki działania dla wszystkich przedsiębiorstw prowadzących działalność na rynku UE**. Rozporządzenie zawiera wymóg, aby przedsiębiorstwa z siedzibą poza UE oferujące towary i usługi, z którymi wiąże się przetwarzanie danych osobowych, lub monitorujące zachowanie osób fizycznych w Unii stosowały te same przepisy, które stosują przedsiębiorstwa z siedzibą w UE. Przedsiębiorstwa spoza UE prowadzące działalność na jednolitym rynku muszą w określonych okolicznościach wyznaczyć

[6] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_pl.pdf

przedstawiciela w UE, do którego obywatele i organy mogą zwracać się oprócz lub zamiast do danego przedsiębiorstwa z siedzibą za granicą;

- **zasada uwzględniania ochrony danych w fazie projektowania i zasada domyślnej ochrony danych**, które stwarzają zachęty do przyjmowania innowacyjnych rozwiązań związanych z ochroną danych już w fazie początkowej;

- **wzmocnione prawa osób fizycznych.** W rozporządzeniu wprowadzono: nowe wymogi w zakresie przejrzystości; wzmocnione prawo do informacji, prawo dostępu i prawo do usunięcia danych („prawo do bycia zapomnianym"); zasadę, zgodnie z którą milczenie lub niepodjęcie działania nie będzie już uznawane za ważne wyrażenie zgody, ponieważ dla wyrażenia zgody wymagane będzie wyraźne działanie potwierdzające; ochronę dzieci w internecie;

- **większa kontrola sprawowana przez osoby fizyczne nad ich danymi osobowymi.** W rozporządzeniu ustanowiono **nowe prawo do przenoszenia danych** umożliwiające obywatelom zażądanie od przedsiębiorstwa lub organizacji, aby przesłały z powrotem dane osobowe dostarczone temu przedsiębiorstwu lub tej organizacji przez dane osoby fizyczne za ich własną zgodą lub na podstawie umowy. Na podstawie tego prawa możliwe będzie również bezpośrednie przekazywanie danych innemu przedsiębiorstwu lub innej organizacji, o ile jest to technicznie możliwe. Prawo do przenoszenia danych umożliwia przesłanie danych osobowych przez jedno przedsiębiorstwo lub jedną organizację bezpośrednio innemu przedsiębiorstwu lub innej organizacji, w związku z czym prawo to wesprze również swobodny przepływ danych osobowych w UE, będzie zapobiegać blokadzie danych osobowych i będzie sprzyjać konkurencji między przedsiębiorstwami. Ułatwienie obywatelom zmiany dostawców usług będzie sprzyjać rozwojowi nowych usług w kontekście strategii jednolitego rynku cyfrowego;

- **wzmocniona ochrona przed naruszeniami ochrony danych**. W rozporządzeniu ustanowiono kompleksowy zestaw przepisów dotyczących naruszeń ochrony danych osobowych. Wyraźnie określono w nim, czym jest „naruszenie ochrony danych osobowych", a także wprowadzono obowiązek zgłoszenia naruszenia organowi nadzorczemu nie później niż w terminie 72 godzin po jego stwierdzeniu w sytuacjach, w których dane naruszenie ochrony danych może powodować ryzyko naruszenia praw lub wolności osób fizycznych. W określonych okolicznościach w rozporządzeniu zobowiązano do powiadomienia o naruszeniu osobę fizyczną, której danych dotyczy dane naruszenie. Pozwala to znacznie wzmocnić ochronę w porównaniu z obecną sytuacją w UE, w której jedynie dostawcy usług łączności elektronicznej, operatorzy usług kluczowych i dostawcy usług cyfrowych są obowiązani do zgłaszania naruszeń ochrony danych na podstawie odpowiednio dyrektywy o prywatności i łączności elektronicznej[7] i dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych[8];

---

[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. 37–47. Zgodnie z art. 95 ogólnego rozporządzenia o ochronie danych rozporządzenie to nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE. Oznacza to na przykład, że podmioty objęte dyrektywą o prywatności i łączności elektronicznej są objęte przewidzianym w tej dyrektywie obowiązkiem zgłaszania naruszenia danych osobowych w zakresie, w jakim naruszenie dotyczy usługi objętej tą dyrektywą. W tym

- **na mocy rozporządzenia wszystkim organom ochrony danych nadano uprawnienie do nakładania kar pieniężnych na administratorów i podmioty przetwarzające.** Obecnie nie wszystkie organy ochrony danych mają takie uprawnienie. Usprawni to wykonywanie przepisów. Kary pieniężne mogą sięgać kwoty 20 mln EUR lub, w przypadku przedsiębiorstwa – 4 % jego rocznego światowego obrotu;

- **większa elastyczność administratorów i podmiotów przetwarzających dane osobowe za sprawą jednoznacznych przepisów dotyczących odpowiedzialności (zasada rozliczalności).** W rozporządzeniu zdecydowano się odejść od systemu zawiadamiania na rzecz zasady rozliczalności. Zasadę rozliczalności wykonuje się w drodze skalowalnych obowiązków w zależności od ryzyka (np. obecność inspektora ochrony danych lub obowiązek przeprowadzania ocen skutków dla ochrony danych). Wprowadzono nowe narzędzie, które pomoże w przeprowadzeniu oceny ryzyka przed rozpoczęciem przetwarzania danych: ocena skutków dla ochrony danych. Ta ostatnia jest wymagana, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. W rozporządzeniu wyraźnie wymieniono trzy sytuacje, w których zachodzi taka konieczność: gdy przedsiębiorstwo prowadzi systematyczną i kompleksową ocenę czynników osobowych odnoszących się do osób fizycznych (w tym profilowanie), przetwarza na dużą skalę dane wrażliwe lub systematycznie monitoruje na dużą skalę miejsca dostępne publicznie. Krajowe organy ochrony danych będą musiały podawać do publicznej wiadomości wykazy sytuacji podlegających wymogowi dokonania oceny skutków dla ochrony danych[9];

- **większa przejrzystość w zakresie obowiązków podmiotów przetwarzających i odpowiedzialności administratorów w momencie wyboru podmiotu przetwarzającego;**

- **nowoczesny system zarządzania zapewniający bardziej konsekwentne i zdecydowane egzekwowanie przepisów.** Obejmuje to zharmonizowane uprawnienia organów ochrony danych – w tym w zakresie kar pieniężnych – oraz nowe mechanizmy współpracy między tymi organami w ramach sieci;

- **w rozporządzeniu zapewniono utrzymanie wysokiego stopnia ochrony danych osobowych przy ich przekazywaniu poza UE**[10]. Chociaż zasadniczo utrzymano strukturę przepisów dotyczących międzynarodowego przekazywania danych zastosowaną w dyrektywie z 1995 r., to jednak w ramach reformy wyjaśniono i uproszczono ich stosowanie oraz wprowadzono nowe narzędzia w zakresie przekazywania danych. Jeżeli chodzi o decyzje stwierdzające odpowiedni stopień ochrony, w rozporządzeniu

---

zakresie ogólne rozporządzenie o ochronie danych nie nakłada na te podmioty żadnych dodatkowych obowiązków.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U. L 194 z 19.7.2016, s. 1–30. Podmioty objęte zakresem stosowania dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych powinny zgłaszać incydenty mające istotny lub znaczny wpływ na świadczenie niektórych ich usług. Zgłaszanie incydentów na podstawie dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych pozostaje bez uszczerbku dla zgłaszania naruszeń na podstawie rozporządzenia.

[9] Art. 35 rozporządzenia.

[10] Komunikat Komisji „Wymiana i ochrona danych osobowych w zglobalizowanym świecie”, COM(2017) 7 final.

wprowadzono precyzyjny i szczegółowy katalog elementów, które Komisja musi uwzględnić przy ocenie kwestii, czy dany zagraniczny system zapewnia odpowiedni poziom ochrony danych osobowych. W rozporządzeniu formalizuje się również alternatywne instrumenty przekazywania danych, takie jak standardowe klauzule umowne i wiążące reguły korporacyjne, oraz zwiększa ich liczbę.

Dzięki przyjęciu zmienionego rozporządzenia dotyczącego unijnych instytucji, organów i jednostek organizacyjnych[11] i rozporządzenia w sprawie prywatności i łączności elektronicznej[12], które obecnie znajdują się na etapie negocjacji, UE zostanie wyposażona w silny i kompleksowy zestaw przepisów o ochronie danych[13].

2. PRACE PRZYGOTOWAWCZE PRZEPROWADZONE DOTYCHCZAS NA SZCZEBLU UE

Skuteczne stosowanie rozporządzenia wymaga współpracy między wszystkimi podmiotami zaangażowanymi w ochronę danych: państwami członkowskimi, w tym organami administracji publicznej, krajowymi organami ochrony danych, przedsiębiorstwami, organizacjami zajmującymi się przetwarzaniem danych osobowych oraz osobami fizycznymi, a także Komisją.

2.1. Działania podejmowane przez Komisję Europejską

W połowie 2016 r., krótko po wejściu rozporządzenia w życie, Komisja nawiązała dialog z organami państw członkowskich, organami ochrony danych i zainteresowanymi stronami w celu przygotowania ich do stosowania rozporządzenia oraz zapewnienia wsparcia i udzielenia wskazówek.

a) Wspieranie państw członkowskich i ich organów

Komisja bardzo ściśle współpracuje z państwami członkowskimi, aby wesprzeć ich działania podczas okresu przejściowego celem zapewnienia najwyższego możliwego poziomu spójności. W tym celu Komisja utworzyła grupę ekspertów, która ma pomagać państwom członkowskim w ich wysiłkach na rzecz przygotowania się do wejścia rozporządzenia w życie. Grupa ta, która odbyła już 13 spotkań, ma charakter forum, na którym państwa członkowskie mogą dzielić się swoimi doświadczeniami i wiedzą fachową[14]. Komisja zorganizowała również dwustronne spotkania z organami państw członkowskich w celu omówienia kwestii pojawiających się na szczeblu krajowym.

---

[11] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylający rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE, COM(2017) 8 final.

[12] 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.

[13] Do czasu przyjęcia i wejścia w życie rozporządzenia w sprawie prywatności i łączności elektronicznej dyrektywa 2002/58/WE ma zastosowanie jako *lex specialis* względem rozporządzenia.

[14] Pełen wykaz spotkań, porządki obrad, streszczenia przeprowadzonych dyskusji i przegląd aktualnej sytuacji w zakresie przepisów obowiązujących w różnych państwach członkowskich można znaleźć pod adresem: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=PL

b) Wspieranie poszczególnych organów ochrony danych i utworzenie Europejskiej Rady Ochrony Danych

Komisja aktywnie wspiera prace Grupy Roboczej Art. 29, mając na uwadze również zapewnienie sprawnego przejścia do funkcjonowania Europejskiej Rady Ochrony Danych[15].

c) Działania na arenie międzynarodowej

Rozporządzenie pozwoli jeszcze bardziej wzmocnić zdolność UE do aktywnego propagowania reprezentowanych przez nią wartości w zakresie ochrony danych, a także ułatwić transgraniczne przepływy danych poprzez wspieranie ujednolicania systemów prawnych w skali światowej[16]. Na forum międzynarodowym coraz częściej uznaje się, że unijne przepisy o ochronie danych wyznaczają najwyższe standardy ochrony danych na świecie. Prowadzone są również prace nad unowocześnieniem Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, która jest jedynym prawnie wiążącym, wielostronnym instrumentem w obszarze ochrony danych osobowych. Komisja dąży do tego, aby konwencja odzwierciedlała te same zasady, które zapisano w nowych unijnych przepisach o ochronie danych, co przyczyni się do ustanowienia jednolitego zestawu wysokich standardów ochrony danych. Komisja będzie aktywnie wspierać szybkie przyjęcie zaktualizowanego tekstu konwencji ze względu na perspektywę przystąpienia UE do tej konwencji[17]. Komisja zachęca państwa trzecie do ratyfikacji Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych i jej protokołu dodatkowego.

Ponadto niektóre kraje i organizacje regionalne spoza UE – począwszy od tych będących w naszym bezpośrednim sąsiedztwie, aż po te, które znajdują się w Azji, Ameryce Łacińskiej i Afryce – przyjmują nowe przepisy w dziedzinie ochrony danych lub aktualizują przepisy już obowiązujące, aby w ten sposób wykorzystać możliwości, jakie daje światowa gospodarka cyfrowa, a także aby odpowiedzieć na rosnące zapotrzebowanie na poprawę bezpieczeństwa danych i ochrony prywatności. Poszczególne państwa różnią się wprawdzie pod względem stosowanego podejścia i stopnia zaawansowania procesu legislacyjnego, można jednak zauważyć oznaki sugerujące, że rozporządzenie w coraz większym stopniu służy za punkt odniesienia i źródło inspiracji[18].

W tym kontekście Komisja prowadzi działania na arenie międzynarodowej zgodnie ze swoim komunikatem ze stycznia 2017 r.[19], aktywnie angażując się we współpracę z kluczowymi partnerami, zwłaszcza w Azji Wschodniej i Południowo-Wschodniej oraz Ameryce

---

[15] Przykładowo Komisja zapewni Europejskiej Radzie Ochrony Danych możliwość wykorzystania systemu wymiany informacji na rynku wewnętrznym (IMI) do komunikacji między jej członkami.

[16] Dokument otwierający debatę w sprawie wykorzystania możliwości płynących z globalizacji, COM(2017) 240.

[17] 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). Do konwencji mogą przystąpić państwa niebędące członkami Rady Europy i ratyfikowało ją już 51 państw (w tym Urugwaj, Mauritius, Senegal i Tunezja).

[18] Zob. np. „Standardy ochrony danych państw iberoamerykańskich", http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

[19] COM(2017) 7.

Łacińskiej, dążąc do rozpoznania możliwości przyjęcia decyzji stwierdzających odpowiedni stopień ochrony[20].

W szczególności Komisja współpracuje z Japonią w zakresie osiągnięcia celu, jakim jest równoczesne uznanie przez obie strony odpowiedniego stopnia ochrony nie później niż do początku 2018 r., zgodnie z treścią wspólnego oświadczenia przewodniczącego Jeana-Claude'a Junckera i premiera Shinzo Abe z dnia 6 lipca 2017 r.[21]. Rozpoczęto również rozmowy z Republiką Korei dotyczące możliwego przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony. Przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony zapewniłoby swobodny przepływ danych w zainteresowanych państwach trzecich, przy jednoczesnym zagwarantowaniu niezbędnego stopnia ochrony danych osobowych przesyłanych z UE do tych krajów.

Jednocześnie Komisja współpracuje z zainteresowanymi stronami w celu wykorzystania pełnego potencjału zestawu narzędzi oferowanych przez ogólne rozporządzenie o ochronie danych na potrzeby międzynarodowego przekazywania danych, opracowując alternatywne mechanizmy przekazywania danych, które będą dopasowane do szczególnych potrzeb lub sytuacji poszczególnych branż lub podmiotów gospodarczych[22].

d) Współpraca z zainteresowanymi stronami

Komisja zorganizowała szereg wydarzeń mających na celu dotarcie do zainteresowanych stron[23]. Na pierwszy kwartał 2018 r. planowane są nowe warsztaty skierowane do konsumentów. Odbyły się również tematyczne dyskusje sektorowe na temat dziedzin takich jak badania i usługi finansowe.

Komisja utworzyła również grupę różnych zainteresowanych stron ds. rozporządzenia złożoną z przedstawicieli organizacji społeczeństwa obywatelskiego, biznesu, środowisk akademickich i osób zajmujących się przedmiotowymi zagadnieniami od strony praktycznej. Grupa ta będzie doradzać Komisji w szczególności w kwestii sposobów osiągnięcia przez zainteresowane strony odpowiedniego poziomu świadomości w zakresie rozporządzenia[24].

Ponadto Komisja Europejska, za pośrednictwem swojego programu ramowego w zakresie badań naukowych i innowacji „Horyzont 2020"[25], finansuje działania na rzecz opracowywania narzędzi wspierających skuteczne stosowanie przepisów dotyczących wyrażania zgody, które przewidziano w rozporządzeniu, oraz działania dotyczące zapewniających ochronę danych metod analizy danych, takich jak obliczanie wielostronne i szyfrowanie homomorficzne.

2.2. Działania prowadzone przez Grupę Roboczą Art. 29 / Europejską Radę Ochrony Danych

[20] COM(2017) 7, tamże s. 10–11.
[21] http://europa.eu/rapid/press-release_STATEMENT-17-1917_en.htm
[22] COM(2017) 7, tamże s. 10–11.
[23] Dwa warsztaty z udziałem przedstawicieli branży w lipcu 2016 r. i kwietniu 2017 r., dwa wydarzenia polegające na rozmowach przy okrągłym stole na tematy biznesowe w grudniu 2016 r. i maju 2017 r., warsztaty na temat danych dotyczących zdrowia w październiku 2017 r. oraz warsztaty z udziałem przedstawicieli MŚP w listopadzie 2017 r.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537
[25] https://ec.europa.eu/programmes/horizon2020/h2020-sections

Grupa Robocza Art. 29 – w skład której wchodzą wszystkie krajowe organy ochrony danych, w tym Europejski Inspektor Ochrony Danych – odgrywa istotną rolę w przygotowaniu do stosowania rozporządzenia poprzez przygotowywanie wytycznych dla przedsiębiorstw i zainteresowanych stron. Ponieważ krajowe organy ochrony danych egzekwują stosowanie rozporządzenia i stanowią główny punkt kontaktu dla zainteresowanych stron, są one w stanie najlepiej zapewnić większą pewność prawa w kwestii interpretacji rozporządzenia.

Wytyczne / dokumenty robocze przygotowane przez Grupę Roboczą Art. 29 na potrzeby rozpoczęcia stosowania rozporządzenia[26]	
Prawo do przenoszenia danych	Przyjęto w dniach 4–5 kwietnia 2017 r.
Inspektorzy ochrony danych	
Wyznaczenie wiodącego organu nadzorczego	
Ocena skutków dla ochrony danych	Przyjęto w dniach 3–4 października 2017 r.
Administracyjne kary pieniężne	Przyjęto w dniach 3–4 października 2017 r.
Profilowanie	Prace w toku
Naruszenia ochrony danych osobowych	Prace w toku
Zgoda	Prace w toku
Przejrzystość	Prace w toku
Certyfikacja i akredytacja	Prace w toku
Odpowiedni stopień ochrony przekazywanych danych osobowych	Prace w toku
Wiążące reguły korporacyjne dla administratorów danych	Prace w toku
Wiążące reguły korporacyjne dla przetwarzających	Prace w toku

Grupa Robocza Art. 29 pracuje nad aktualizacją istniejących opinii, w tym dotyczących narzędzi przesyłania danych do państw trzecich.

Ponieważ niezbędne jest, aby podmioty gospodarcze miały dostęp do spójnego i jednolitego zestawu wytycznych, obecne wytyczne na szczeblu krajowym muszą zostać albo uchylone, albo dostosowane do przyjętych przez Grupę Roboczą Art. 29 / Europejską Radę Ochrony Danych wytycznych dotyczących tych samych zagadnień.

Komisja przywiązuje szczególną wagę do objęcia wytycznych konsultacjami publicznymi przed finalizacją. Konieczne jest, aby wkład zainteresowanych stron w ten proces był jak najdokładniejszy i jak najkonkretniejszy, co pomoże we wskazaniu najlepszych praktyk i zwróci uwagę Grupy Roboczej Art. 29 na cechy branżowe i sektorowe. Ostateczna

[26] Wszystkie przyjęte wytyczne są dostępne pod adresem: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

odpowiedzialność za te wytyczne spoczywa na Grupie Roboczej Art. 29 i przyszłej Europejskiej Radzie Ochrony Danych, i to do nich organy ochrony danych będą zwracać się podczas egzekwowania rozporządzenia.

Powinna istnieć możliwość zmiany wytycznych ze względu na rozwój sytuacji i stosowane praktyki. W związku z tym ważne jest, aby organy ochrony danych promowały kulturę dialogu ze wszystkimi zainteresowanymi stronami, w tym z przedsiębiorstwami.

Należy pamiętać, że jeżeli pojawią się wątpliwości dotyczące stosowania rozporządzenia, ostateczną interpretację rozporządzenia zapewnią sądy na szczeblach krajowym i unijnym.

3. POZOSTAŁE DZIAŁANIA, KTÓRYCH WYMAGA SKUTECZNE PRZYGOTOWANIE

3.1. Finalizacja ustanawiania ram prawnych na szczeblu krajowym przez państwa członkowskie

Rozporządzenie ma bezpośrednie zastosowanie we wszystkich państwach członkowskich[27]. Oznacza to, że rozporządzenie wchodzi w życie i jest stosowane bez względu na istniejące środki prawodawstwa krajowego: bezpośrednio do przepisów rozporządzenia mogą z reguły odwoływać się obywatele, przedsiębiorstwa, administracje publiczne i inne organizacje zajmujące się przetwarzaniem danych osobowych. Państwa członkowskie muszą jednak – zgodnie z rozporządzeniem – podjąć działania niezbędne do dostosowania swojego ustawodawstwa, a mianowicie: uchylić i zmienić obowiązujące przepisy, utworzyć krajowe organy ochrony danych[28], wybrać jednostkę akredytującą[29] oraz ustanowić przepisy mające na celu pogodzenie wolności wypowiedzi z ochroną danych[30].

Dzięki rozporządzeniu państwa członkowskie uzyskały również możliwość dalszego doprecyzowania stosowania przepisów o ochronie danych w określonych dziedzinach: sektora publicznego[31], prawa pracy i zabezpieczenia społecznego[32], profilaktyki zdrowotnej lub medycyny pracy, zdrowia publicznego[33], przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych[34], krajowego numeru identyfikacyjnego[35], publicznego dostępu do dokumentów urzędowych[36],

---

[27] Art. 288 TFUE.

[28] Art. 54 ust. 1 rozporządzenia.

[29] Zgodnie z art. 43 ust. 1 rozporządzenia państwa członkowskie umożliwiają podmiotom certyfikującym skorzystanie z dwóch sposobów akredytacji, tj. przez krajowy organ nadzorujący ochronę danych utworzony na mocy przepisów w dziedzinie ochrony danych lub przez krajową jednostkę akredytującą utworzoną na mocy rozporządzenia (WE) nr 765/2008 dotyczącego akredytacji i nadzoru rynku. W tym celu Europejska Współpraca w Dziedzinie Akredytacji („EA", uznana na mocy rozporządzenia nr 765/2008), w której skład wchodzą krajowe jednostki akredytujące, oraz organy nadzorcze określone w RODO powinny ściśle ze sobą współpracować.

[30] Art. 85 ust. 1 rozporządzenia.

[31] Art. 6 ust. 2 rozporządzenia.

[32] Art. 88 oraz 9 ust. 2 lit. b) rozporządzenia. Europejski filar praw socjalnych stanowi również, że „pracownicy mają prawo do ochrony swoich danych osobowych w kontekście zatrudnienia" (2017/C 428/09, Dz.U. C 428 z 13.12.2017, s. 10–15).

[33] Art. 9 ust. 2 lit. h) oraz i) rozporządzenia.

[34] Art. 9 ust. 2 lit. j) rozporządzenia.

[35] Art. 87 rozporządzenia.

[36] Art. 86 rozporządzenia.

i obowiązku zachowania tajemnicy[37]. Ponadto rozporządzenie uprawnia państwa członkowskie do zachowania lub wprowadzania dalszych warunków, w tym ograniczeń, przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia[38].

Działania państw członkowskich w tym kontekście są ograniczone przez dwa elementy:

1. art. 8 Karty, co oznacza, że wszelkie krajowe przepisy doprecyzowujące muszą spełniać wymogi określone w art. 8 Karty (oraz rozporządzenia, które opiera się na art. 8 Karty); oraz
2. art. 16 ust. 2 TFUE, zgodnie z którym przepisy krajowe nie mogą naruszać swobodnego przepływu danych osobowych w UE.

Rozporządzenie daje możliwość uproszczenia otoczenia prawnego, czyli zmniejszenia liczby przepisów krajowych i zapewnienia podmiotom większej przejrzystości.

Dostosowując swoje przepisy krajowe, państwa członkowskie muszą wziąć pod uwagę fakt, że wszelkie działania na szczeblu krajowym, które mogłyby stworzyć przeszkody dla bezpośredniego stosowania rozporządzenia i które mogłyby zagrozić jego jednoczesnemu i jednolitemu stosowaniu w całej UE, są sprzeczne z Traktatami[39].

Zakazane jest ponadto powtarzanie treści rozporządzeń w prawie krajowym (np. powtarzanie definicji lub praw osób fizycznych), chyba że takie powtórzenia są absolutnie niezbędne, aby spójność była zachowana oraz aby przepisy krajowe były zrozumiałe dla osób, do których mają zastosowanie[40]. Dosłowne powielenie treści rozporządzenia w prawie krajowym powinno stanowić wyjątek i być uzasadnione, przy czym nie można go stosować w celu wprowadzenia dodatkowych warunków lub interpretacji do treści rozporządzenia.

Wykładnię rozporządzenia pozostawia się sądom europejskim (sądom krajowym i ostatecznie Trybunałowi Sprawiedliwości), nie prawodawcom państw członkowskich. Ustawodawca krajowy nie może zatem kopiować treści rozporządzenia, jeżeli nie jest to konieczne w świetle kryteriów określonych w orzecznictwie, ani interpretować czy wprowadzać dodatkowych warunków do przepisów mających bezpośrednie zastosowanie na mocy rozporządzenia. W takim przypadku podmioty gospodarcze w Unii byłyby bowiem znów narażone na rozdrobnienie i nie wiedziałyby, do których przepisów mają się stosować.

Na tym etapie jedynie dwa państwa członkowskie przyjęły odpowiednie ustawodawstwo krajowe[41]; w pozostałych państwach członkowskich procedura ustawodawcza znajduje się na różnych etapach zaawansowania[42], państwa te przewidziały przyjęcie odpowiedniego

---

[37] Art. 90 rozporządzenia.
[38] Art. 9 ust. 4 rozporządzenia.
[39] Wyrok Trybunału z dnia 31 stycznia 1978 r., Fratelli Zerbone Snc przeciwko Amministrazione delle finanze dello Stato, C-94/77, ECLI:EU:C:1978:17 oraz 101.
[40] Motyw 8 rozporządzenia.
[41] Austria (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Niemcy (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1513091793362).
[42] Przegląd aktualnego stanu prac nad procesem legislacyjnym w poszczególnych państwach członkowskich jest dostępny pod adresem:

ustawodawstwa do dnia 25 maja 2018 r. Istotne jest, aby podmioty gospodarcze miały wystarczająco dużo czasu na przygotowanie się do wprowadzenia wszystkich przepisów, których będą musiały przestrzegać.

Jeżeli państwa członkowskie nie podejmą działań wymaganych na podstawie rozporządzenia, opóźnią się w ich podjęciu lub wykorzystają określone w rozporządzeniu klauzule precyzujące w sposób sprzeczny z rozporządzeniem, Komisja skorzysta ze wszystkich dostępnych narzędzi, w tym z możliwości wszczęcia postępowania w sprawie naruszenia.

3.2. Zapewnienie pełnej operacyjności nowej niezależnej Europejskiej Rady Ochrony Danych przez organy ochrony danych

Zasadnicze znaczenie ma, aby nowy organ utworzony na mocy rozporządzenia, tj. Europejska Rada Ochrony Danych[43], następca Grupy Roboczej Art. 29, osiągnął pełną zdolność operacyjną do dnia 25 maja 2018 r.

Mając na celu wzmocnienie synergii i skuteczności, Europejski Inspektor Ochrony Danych, tj. organ ochrony danych odpowiedzialny za nadzór instytucji i organów UE, zadba o sekretariat Europejskiej Rady Ochrony Danych. W tym celu w minionych miesiącach Europejski Inspektor Ochrony Danych rozpoczął niezbędne przygotowania.

Europejska Rada Ochrony Danych znajdzie się w centrum ochrony danych w Europie. Będzie ona przyczyniać się do jednolitego stosowania prawa w dziedzinie ochrony danych oraz zapewni silną podstawę współpracy między organami ochrony danych, w tym Europejskiego Inspektora Ochrony Danych. Europejska Rada Ochrony Danych będzie nie tylko wydawać wytyczne w sprawie interpretacji kluczowych pojęć rozporządzenia, ale będzie również wydawać wiążące decyzje w sporach dotyczących transgranicznego przetwarzania. Zapewni to jednolite stosowanie przepisów unijnych i zapobiegnie rozstrzyganiu tej samej sprawy w rozbieżny sposób w różnych państwach członkowskich.

Sprawne i efektywne funkcjonowanie Europejskiej Rady Ochrony Danych jest zatem warunkiem dobrego funkcjonowania systemu jako całości. Dla zapewnienia jednolitej interpretacji przepisów rozporządzenia Europejska Rada Ochrony Danych będzie musiała stworzyć wspólną kulturę ochrony danych wśród wszystkich krajowych organów ochrony danych, co będzie zadaniem intensywniejszym niż kiedykolwiek wcześniej. Rozporządzenie sprzyja współpracy między organami ochrony danych, nadając im narzędzia do skutecznej i efektywnej współpracy: w szczególności będą one w stanie przeprowadzać wspólne operacje, przyjmować decyzje w ramach porozumienia oraz rozstrzygać potencjalne rozbieżności dotyczące interpretacji rozporządzenia na forum Rady w drodze opinii i wiążących decyzji. Komisja zachęca organy ochrony danych do przyjęcia tych zmian i dostosowania swojej kultury funkcjonowania, finansowania i pracy, aby móc przyjąć nowe prawa i spełniać nowe obowiązki.

3.3. Zapewnienie przez państwa członkowskie niezbędnych zasobów finansowych i ludzkich na potrzeby organów ochrony danych

---

http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=PL

[43] Europejska Rada Ochrony Danych będzie organem UE posiadającym osobowość prawną i odpowiedzialnym za jednolite stosowanie rozporządzenia. W skład tego organu wchodzić będą przewodniczący wszystkich organów ochrony danych oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele.

Utworzenie w pełni niezależnych organów nadzorczych w każdym państwie członkowskim ma kluczowe znaczenie dla zapewnienia ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych w UE[44]. Organy nadzorcze nie mogą skutecznie chronić praw i wolności osób fizycznych, jeżeli nie są całkowicie niezależne. Jakiekolwiek uchybienie przy gwarantowaniu im niezależności i nadawaniu uprawnień ma daleko idący, negatywny wpływ na wykonywanie przepisów z zakresu ochrony danych[45].

W rozporządzeniu skodyfikowano wymóg, zgodnie z którym wszystkie organy ochrony danych mają działać w sposób całkowicie niezależny[46]. Zwiększa on niezależność krajowych organów ochrony danych i nadaje im jednolite uprawnienia w całej UE, tak aby posiadały one odpowiednie kompetencje do skutecznego rozpatrywania skarg, uprawnienia do przeprowadzania skutecznych dochodzeń, podejmowania wiążących decyzji i nakładania skutecznych i odstraszających sankcji. Nadano im ponadto uprawnienia do nakładania administracyjnych kar pieniężnych na administratorów czy podmioty przetwarzające w wysokości do 20 mln EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Organy ochrony danych są naturalnymi partnerami i pierwszym punktem kontaktowym dla ogółu społeczeństwa, przedsiębiorstw i administracji publicznych w przypadku pytań dotyczących rozporządzenia. Rola organów ochrony danych obejmuje informowanie administratorów i podmiotów przetwarzających o ich zobowiązaniach, a także upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz zrozumienia tych zjawisk. Nie oznacza to jednak, że administratorzy i podmioty przetwarzające powinni oczekiwać, że organy ochrony danych zapewnią im dostosowaną do potrzeb, zindywidualizowaną opinię prawną, którą zapewnić może jedynie prawnik bądź inspektor ochrony danych.

Krajowe organy ochrony danych odgrywają kluczową rolę, jednak stosunkowy brak równowagi między zasobami ludzkimi i finansowymi, które przydziela się im w różnych państwach członkowskich, może stanowić zagrożenie dla ich skuteczności, a ostatecznie – dla ich pełnej niezależności wymaganej na podstawie rozporządzenia. Może to również mieć negatywny wpływ na sposób, w jaki organy ochrony danych mogą wykonywać swoje uprawnienia, takie jak uprawnienia w zakresie prowadzenia dochodzeń. Zachęca się państwa członkowskie do wypełnienia ich prawnego obowiązku, jakim jest zapewnienie krajowym organom ochrony danych zasobów kadrowych, technicznych i finansowych, pomieszczeń i infrastruktury niezbędnych do skutecznego wypełniania ich zadań i wykonywania ich uprawnień[47].

3.4. Przygotowywanie się przedsiębiorstw, administracji publicznych i innych organizacji przetwarzających dane do stosowania nowych przepisów

Rozporządzenie nie zmieniło w znaczący sposób głównych pojęć i zasad dotyczących przepisów w dziedzinie ochrony danych wprowadzonych w 1995 r. Oznacza to, że znaczna większość administratorów i podmiotów przetwarzających nie będzie musiała wprowadzać

[44] Motyw 117 i wcześniejsze stwierdzenie już w motywie 62 dyrektywy 95/46.

[45] Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, COM(2007) 87 final z dnia 7 marca 2007 r.

[46] Art. 52 rozporządzenia.

[47] Art. 52 ust. 4 rozporządzenia.

istotnych zmian w operacjach przetwarzania danych w celu osiągnięcia zgodności z rozporządzeniem, pod warunkiem, że już teraz działają oni zgodnie z obowiązującymi w UE przepisami w zakresie ochrony danych.

Rozporządzenie ma wpływ przede wszystkim na podmioty gospodarcze, których główną działalnością gospodarczą jest przetwarzanie danych lub obchodzenie się z danymi wrażliwymi. Ma również wpływ na podmioty, które regularnie i systematycznie monitorują osoby fizyczne na dużą skalę. Te podmioty gospodarcze będą najprawdopodobniej musiały wyznaczyć inspektora ochrony danych, przeprowadzić ocenę skutków dla ochrony danych i zgłosić naruszenia ochrony danych, jeżeli istnieje zagrożenie dla praw i wolności osób fizycznych. Dla porównania, podmioty gospodarcze – w szczególności MŚP – których główna działalność nie obejmuje przetwarzania, z którym łączy się wysokie ryzyko, co do zasady nie podlegają wspomnianym szczególnym zobowiązaniom określonym w rozporządzeniu.

Istotne jest, aby administratorzy i podmioty przetwarzające podejmowali się dogłębnych przeglądów cyklu swojej polityki w zakresie danych, aby mogli wyraźnie zidentyfikować, jakie dane posiadają, do jakich celów i na jakiej podstawie prawnej (np. chmura; podmioty gospodarcze w sektorze finansowym). Muszą oni również dokonać oceny obowiązujących umów, w szczególności tych zawartych między administratorami i podmiotami przetwarzającymi, ścieżek międzynarodowego przekazywania danych i ogólnego zarządzania (stosowanych środków informatycznych i organizacyjnych), w tym wyznaczenia inspektora ochrony danych. Zasadniczym elementem w tym procesie jest zapewnienie, aby w takich przeglądach brał udział najwyższy szczebel zarządzania, wnosił swój wkład oraz aby regularnie przekazywano mu najnowsze informacje i konsultowano się z nim w sprawie zmian dotyczących polityki danych przedsiębiorstwa.

W tym celu niektóre podmioty gospodarcze korzystają z list kontrolnych odnoszących się do zgodności (wewnętrznych albo zewnętrznych), konsultują się z przedsiębiorstwami doradczymi i kancelariami prawnymi oraz poszukują produktów, które spełnią wymogi w zakresie uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Każdy sektor musi wypracować ustalenia odpowiednie do szczególnego charakteru swojej dziedziny i dostosowane do danego modelu biznesowego.

Przedsiębiorstwa i inne organizacje przetwarzające dane będą mogły wykorzystać nowe narzędzia przewidziane w rozporządzeniu również jako element wykazania zgodności, np. kodeksy postępowania i mechanizmy certyfikacji. Chodzi to o podejścia oddolne, które wywodzą się ze środowiska biznesu, stowarzyszeń i innych organizacji reprezentujących kategorie administratorów i podmiotów przetwarzających oraz odzwierciedlają najlepsze praktyki, istotne zmiany w danym sektorze, lub które mogą informować o poziomie ochrony danych wymaganym przez niektóre produkty i usługi. W rozporządzeniu przewidziano uproszczony zbiór przepisów dotyczących takich mechanizmów, biorąc pod uwagę realia rynkowe (np. certyfikacje udzielone przez podmiot certyfikujący lub przez organ ochrony danych).

Wprawdzie duże przedsiębiorstwa czynnie przygotowują się do stosowania nowych przepisów, jednak wiele MŚP nie jest w pełni świadomych nadchodzących przepisów o ochronie danych.

Krótko mówiąc, podmioty gospodarcze powinny przygotować i dostosować się do nowych przepisów oraz postrzegać rozporządzenie jako:

- możliwość przywrócenia prawidłowości w funkcjonowaniu przedsiębiorstwa, jeżeli chodzi o rodzaj przetwarzanych danych osobowych i sposób zarządzania nimi;
- zobowiązanie do opracowania produktów sprzyjających prywatności i ochronie danych oraz budowania z klientami nowych relacji opierających się na przejrzystości i zaufaniu; oraz
- możliwość podjęcia na nowo stosunków z organami ochrony danych poprzez rozliczalność i aktywne przestrzeganie przepisów.

3.5. Informowanie zainteresowanych stron, w szczególności obywateli oraz małych i średnich przedsiębiorstw

Powodzenie rozporządzenia zależy od właściwej świadomości wszystkich podmiotów, których dotyczą nowe przepisy (środowiska biznesu i innych organizacji przetwarzających dane, sektora publicznego i obywateli). Jeżeli chodzi o szczebel krajowy, zadanie podnoszenia świadomości i obowiązek stanowienia pierwszego punktu kontaktowego dla administratorów, podmiotów przetwarzających i osób fizycznych należy przede wszystkim do organów ochrony danych. Jako organy egzekwowania przepisów o ochronie danych na swoim terytorium, organy ochrony danych są również najwłaściwsze do wyjaśniania przedsiębiorstwom i sektorowi publicznemu zmian wprowadzonych rozporządzeniem oraz do zapoznania obywateli z ich prawami.

Organy ochrony danych rozpoczęły informowanie zainteresowanych stron zgodnie z odpowiednim podejściem krajowym. Niektóre państwa organizują seminaria z udziałem administracji publicznych, zarówno na szczeblu regionalnym, jak i lokalnym, oraz prowadzą warsztaty dla różnych sektorów gospodarczych w celu podniesienia świadomości w zakresie głównych przepisów rozporządzenia. Niektóre prowadzą tematyczne programy szkoleniowe dla inspektorów ochrony danych. Większość z nich udostępnia na swoich stronach internetowych materiały informacyjne w różnych formatach (listy kontrolne, wideo itp.).

Świadomość zmian i większych praw, które wprowadzą przepisy o ochronie danych, wciąż nie jest jednak wystarczająco rozpowszechniona wśród obywateli. Należy kontynuować i zintensyfikować uruchomioną przez organy ochrony danych inicjatywę na rzecz szkoleń i podnoszenia świadomości, skupiając się przede wszystkim na MŚP. Ponadto krajowe administracje sektorowe mogą wspierać działania organów ochrony danych i – w oparciu o uzyskane od nich informacje – prowadzić własne działania informacyjne skierowane do różnych zainteresowanych stron.

4. KOLEJNE KROKI

W ciągu najbliższych miesięcy Komisja będzie aktywnie wspierać wszystkie podmioty w przygotowaniu do stosowania rozporządzenia.

a) Współpraca z państwami członkowskimi

Komisja będzie kontynuować współpracę z państwami członkowskimi w ramach przygotowania do zmian, które wejdą w życie w maju 2018 r. Począwszy od maja 2018 r. Komisja będzie monitorować sposób stosowania nowych przepisów przez państwa członkowskie i – w razie potrzeby – podejmować odpowiednie działania.

b) Nowe wytyczne dostępne w internecie we wszystkich językach UE i działania związane z podnoszeniem świadomości

Komisja udostępnia praktyczne wytyczne[48], aby pomóc przedsiębiorcom, w szczególności MŚP, a także organom publicznym i społeczeństwu w przestrzeganiu nowych przepisów o ochronie danych i w korzystaniu z nich.

Wytyczne mają postać praktycznego narzędzia internetowego, które jest dostępne we wszystkich językach UE. To narzędzie internetowe będzie regularnie aktualizowane i ma służyć trzem głównym grupom odbiorców docelowych: obywatelom, przedsiębiorstwom (w szczególności MŚP) i innym organizacjom oraz organom administracji publicznej. Zawiera ono pytania i odpowiedzi wybrane na podstawie informacji zwrotnych otrzymanych od zainteresowanych stron, a także praktyczne przykłady i odniesienia do różnych źródeł informacji (np. do artykułów rozporządzenia, wytycznych Grupy Roboczej Art. 29 / Europejskiej Rady Ochrony Danych, jak również do materiałów opracowanych na szczeblu krajowym).

Komisja będzie dokonywać regularnych aktualizacji tego narzędzia, uzupełniając pytania i aktualizując odpowiedzi, w oparciu o otrzymane informacje zwrotne i w świetle wszelkich nowych kwestii pojawiających się w trakcie wdrażania.

Wytyczne będą promowane za pośrednictwem kampanii informacyjnej i działań w zakresie rozpowszechniania prowadzonych we wszystkich państwach członkowskich, skierowanych do przedsiębiorstw i społeczeństwa.

Rozporządzenie przewiduje silniejsze prawa osób fizycznych, Komisja zaangażuje się również w działania z zakresu podnoszenia świadomości i będzie uczestniczyć w wydarzeniach odbywających się w poszczególnych państwach członkowskich, aby informować obywateli o korzyściach płynących z rozporządzenia oraz o jego oddziaływaniu.

c) Wsparcie finansowe dla krajowych kampanii i działań z zakresu podnoszenia świadomości

Komisja wspiera podejmowane na szczeblu krajowym wysiłki mające na celu podnoszenie świadomości i zapewnienie przestrzegania przepisów, przyznając dotacje, które mogą zostać wykorzystane do organizowania szkoleń dla pracowników organów ochrony danych i organów administracji publicznej, przedstawicieli zawodów prawniczych oraz dla inspektorów ochrony danych[49], jak również do zapoznania ich z rozporządzeniem.

Około 1,7 mln EUR zostanie przyznane sześciu beneficjentom, których obszar działania obejmuje ponad połowę państw członkowskich. Finansowanie będzie skierowane do organów publicznych, w tym do inspektorów ochrony danych podlegających pod władze lokalne i organy publiczne, oraz do inspektorów z sektora prywatnego, sędziów i prawników. Dotacje będą wykorzystywane do rozszerzania materiałów szkoleniowych przeznaczonych dla organów ochrony danych, inspektorów ochrony danych i innych specjalistów, a także dla programów szkoleń przeznaczonych dla osób prowadzących szkolenia.

---

[48] Wytyczne przyczynią się do lepszego zrozumienia unijnych przepisów o ochronie danych, ale moc prawną ma jedynie tekst rozporządzenia. A zatem wyłącznie na mocy rozporządzenia można ustanawiać prawa i obowiązki względem osób fizycznych.

[49] Dotacje przyznane w ramach programu „Prawa, równość i obywatelstwo”: https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c,topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

Komisja wystosowała również zaproszenie do składania wniosków skierowane specjalnie do organów ochrony danych. Całkowity budżet dotacji wyniesie do 2 mln EUR, a środki te wspomogą organy ochrony danych w dotarciu do zainteresowanych stron[50]. Mają one na celu zapewnienie współfinansowania – na poziomie 80 % – środków, które będą stosowane przez organy ochrony danych w latach 2018–2019 w celu podnoszenia świadomości wśród przedsiębiorstw, w szczególności MŚP, i odpowiadania na ich pytania. Finansowanie to można wykorzystać również do podnoszenia świadomości w społeczeństwie.

d) Ocena zapotrzebowania na wykorzystanie uprawnień Komisji

Na mocy rozporządzenia[51] Komisja otrzymuje uprawnienie do wydawania aktów wykonawczych lub delegowanych w celu dalszego wsparcia wdrażania nowych przepisów. Komisja będzie korzystać z tych uprawnień tylko wtedy, gdy ich użycie wyraźnie wytworzy wartość dodaną, i w oparciu o informacje zwrotne uzyskane w drodze konsultacji z zainteresowanymi stronami. W szczególności Komisja zbada kwestię certyfikacji, opierając się na badaniu zleconym ekspertom zewnętrznym oraz na informacjach i wskazówkach na ten temat, które uzyskano od grupy reprezentującej różne zainteresowane strony, powołanej ds. rozporządzenia pod koniec 2017 r. W tym kontekście istotne będą również działania podejmowane przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) w dziedzinie cyberbezpieczeństwa.

e) Włączenie rozporządzenia do Porozumienia EOG

Komisja będzie kontynuować współpracę z państwami EFTA (Islandią, Liechtensteinem i Norwegią) w ramach Europejskiego Obszaru Gospodarczego (EOG) w celu włączenia rozporządzenia do Porozumienia EOG[52]. Dopiero kiedy rozporządzenie zostanie prawomocnie włączone do Porozumienia EOG, dane osobowe będą mogły swobodnie przepływać między państwami UE i EOG w taki sam sposób, w jaki przepływają między państwami członkowskimi UE.

f) Wyjście Zjednoczonego Królestwa z UE

W kontekście prowadzonych między UE a Zjednoczonym Królestwem negocjacji w sprawie umowy o wystąpieniu na podstawie art. 50 Traktatu o Unii Europejskiej celem Komisji będzie zapewnienie, aby przepisy prawa Unii o ochronie danych osobowych, które mają zastosowanie w dniu poprzedzającym wystąpienie, w dalszym ciągu miały zastosowanie dla danych osobowych przetworzonych w Zjednoczonym Królestwie przed datą wystąpienia[53].

---

[50] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html

[51] Akt delegowany w sprawie przedstawiania informacji za pomocą znaków graficznych i procedur opracowywania standardowych znaków graficznych (art. 12 ust. 8 rozporządzenia); akt delegowany w sprawie wymogów, które należy uwzględnić w mechanizmie certyfikacji (art. 43 ust. 8 rozporządzenia); akt wykonawczy w sprawie określania technicznych standardów mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposobów upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków jakości i oznaczeń (art. 43 ust. 9 rozporządzenia); akt wykonawczy w sprawie formatu i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi do celów wiążących reguł korporacyjnych (art. 47 ust. 3 rozporządzenia); akty wykonawcze w sprawie formatu i procedur wzajemnej pomocy i wymiany informacji drogą elektroniczną między organami nadzorczymi (art. 61 ust. 9 i art. 67 rozporządzenia).

[52] Aby uzyskać dodatkowe informacje na temat aktualnej sytuacji, zob.: http://www.efta.int/eea-lex/32016R0679

[53] https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

Na przykład osoby fizyczne, których ta sytuacja dotyczy, powinny dalej posiadać prawo do informacji, prawo dostępu, prawo do sprostowania, usunięcia, do ograniczenia przetwarzania, do przenoszenia danych, prawo do sprzeciwu wobec przetwarzania, a także do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu – na podstawie odpowiednich przepisów prawa Unii, które mają zastosowanie w dniu wystąpienia. Wskazane powyżej dane osobowe nie mogą być przechowywane dłużej niż jest to konieczne dla celów, dla których te dane osobowe zostały przetworzone.

Z dniem wystąpienia – oraz przy uwzględnieniu wszelkich przepisów przejściowych, które mogą zostać zawarte w możliwej umowie o wystąpieniu – wobec Zjednoczonego Królestwa będą miały zastosowanie przepisy rozporządzenia dotyczące przekazów danych osobowych do państw trzecich[54].

g) Podsumowanie postępów w maju 2019 r.

Po dniu 25 maja 2018 r. Komisja będzie ściśle monitorować stosowanie nowych przepisów i będzie gotowa do podjęcia działań, jeżeli pojawią się jakiekolwiek znaczące problemy. Po upływie roku od wejścia w życie rozporządzenia (w 2019 r.) Komisja zorganizuje wydarzenie, podczas którego będzie możliwe podsumowanie doświadczeń różnych zainteresowanych stron w zakresie wdrażania rozporządzenia. Te informacje będą również przydatne w sporządzeniu sprawozdania, które Komisja musi opracować do maja 2020 r. i które ma dotyczyć oceny i przeglądu rozporządzenia. Sprawozdanie to skupi się w szczególności na międzynarodowym przekazywaniu danych i na przepisach dotyczących współpracy i spójności, które mają związek z działalnością organów ochrony danych.

Podsumowanie

W dniu 25 maja w całej UE wejdzie w życie nowy jednolity zestaw przepisów o ochronie danych. Nowe ramy przyniosą znaczne korzyści zarówno osobom fizycznym, przedsiębiorstwom, organom administracji publicznej, jak i innym organizacjom. Stwarza to UE także okazję przekształcenia się w światowego lidera ochrony danych osobowych. Niemniej reforma może odnieść sukces tylko wtedy, gdy wszystkie zaangażowane strony zaakceptują swoje obowiązki i swoje prawa.

Od czasu przyjęcia rozporządzenia w maju 2016 r. Komisja prowadziła aktywny dialog ze wszystkimi zainteresowanymi podmiotami: rządami, organami krajowymi, przedsiębiorstwami, organizacjami społeczeństwa obywatelskiego, dotyczący stosowania nowych przepisów. Włożono wprawdzie bardzo dużo pracy w zapewnienie wysokiego poziomu świadomości i pełnej gotowości, jest jednak jeszcze wiele do zrobienia. Państwa członkowskie i różne zainteresowane strony przygotowują się w różnym tempie. Ponadto wiedza na temat korzyści i możliwości, które przynoszą nowe przepisy, nie wszędzie jest tak samo rozpowszechniona. Szczególnie konieczne jest podniesienie świadomości i wsparcie działań na rzecz przestrzegania przepisów przez MŚP.

W związku z tym Komisja wzywa wszystkie zainteresowane strony do zintensyfikowania prowadzonych działań, aby zapewnić spójne stosowanie i interpretację nowych przepisów w całej UE i podnieść świadomość zarówno wśród przedsiębiorstw, jak i obywateli. Komisja

[54] Zobacz zawiadomienie Komisji dla zainteresowanych stron: przepisy dotyczące wyjścia Zjednoczonego Królestwa z UE w dziedzinie ochrony danych (http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

będzie wspierać te wysiłki, zapewniając finansowanie i wsparcie administracyjne. Komisja pomoże także w podnoszeniu ogólnej świadomości, szczególnie poprzez uruchomienie zestawu narzędzi internetowych.

Dane stają się bardzo cenne dla współczesnej gospodarki i są bardzo istotne w codziennym życiu obywateli. Nowe przepisy stanowią wyjątkową szansę zarówno dla przedsiębiorstw, jak i dla społeczeństwa. Przedsiębiorstwa – szczególnie mniejsze – będą mogły skorzystać z jednolitego, sprzyjającego innowacji zestawu przepisów i uporządkować swoje rozwiązania w kwestii danych osobowych, aby odzyskać zaufanie konsumentów i wykorzystać je jako przewagę konkurencyjną w UE. Obywatele skorzystają z silniejszej ochrony danych osobowych i uzyskają większą kontrolę nad sposobem, w jaki przedsiębiorstwa obchodzą się z danymi.

We współczesnym świecie, w którym dokonuje się gwałtowny rozwój gospodarki cyfrowej, Unia Europejska, jej obywatele i przedsiębiorstwa muszą dysponować wyposażeniem umożliwiającym czerpanie korzyści z gospodarki opartej na danych i zrozumienie jej wpływu. Rozporządzenie zapewnia narzędzia niezbędne do przygotowania Europy na XXI wiek.

Komisja podejmie następujące działania:

Wobec państw członkowskich

- Komisja będzie dalej współpracować z państwami członkowskimi w celu wspierania spójności i ograniczenia fragmentacji w stosowaniu rozporządzenia, uwzględniając swobodę w doprecyzowaniu przepisów, którą daje państwom członkowskim nowe prawodawstwo;

- począwszy od maja 2018 r. Komisja będzie ściśle monitorować stosowanie rozporządzenia w państwach członkowskich i w razie potrzeby podejmować odpowiednie działania, w tym działania w odpowiedzi na naruszenia przepisów;

Wobec organów ochrony danych

- do maja 2018 r. Komisja będzie wspierać działania organów ochrony danych w kontekście Grupy Roboczej Art. 29 i okresu przejściowego przed rozpoczęciem funkcjonowania Europejskiej Rady Ochrony Danych; od maja 2018 r. będzie pomagać Europejskiej Radzie Ochrony Danych w jej pracy;

- w latach 2018–2019 Komisja będzie współfinansować (całkowity budżet wyniesie do 2 mln EUR) działania związane z podnoszeniem świadomości prowadzone przez organy ochrony danych na szczeblu krajowym (projekty realizowane od połowy 2018 r.);

Wobec zainteresowanych stron

- Komisja przygotuje praktyczne narzędzie internetowe dostarczające porad, w którym zawarte będą pytania i odpowiedzi ukierunkowane na obywateli, przedsiębiorstwa i organy administracji publicznej. Komisja zamierza promować te wytyczne wśród odbiorców docelowych, prowadząc kampanię informacyjną skierowaną do przedsiębiorstw i społeczeństwa zarówno w okresie poprzedzającym maj 2018 r., jaki

i później;

- w 2018 r. i w latach kolejnych Komisja będzie nadal prowadzić aktywny dialog z zainteresowanymi stronami, szczególnie za pośrednictwem grupy reprezentującej różne zainteresowane strony, dotyczący wdrożenia rozporządzenia i poziomu świadomości w zakresie nowych przepisów;

Wobec wszystkich podmiotów

- w latach 2018–2019 Komisja oceni, czy będzie musiała wykorzystać swoje uprawnienia do przyjmowania aktów delegowanych lub wykonawczych;

- w maju 2019 r. Komisja dokona podsumowania wdrażania rozporządzenia, a w 2020 r. przygotuje sprawozdanie w sprawie stosowania nowych przepisów.