Jacek Bajorek
University of Social Sciences, Warsaw, Poland

Rozporządzenie ogólne o ochronie danych osobowych (RODO) – nowe wyzwania w zakresie ochrony danych osobowych

Abstrakt

Celem artykułu jest przedstawienie i omówienie Rozporządzenia ogólnego o ochronie danych osobowych (RODO), które ma ujednolicić poziom ochrony danych i zapewnić poczucie pewności prawnej w zakresie przetwarzania danych osobowych we wszystkich krajach Unii Europejskiej. RODO nakłada też nowe obowiązki na przedsiębiorców i administrację rządową, wprowadza szereg zmian i nowości o charakterze prawnym i informatycznym, a czas na przygotowanie się do zmian kończy się 25 maja 2018 r. Badania metodologiczne pojawiają się zarówno w związku z wprowadzeniem Rozporządzenia, jak i samym procesem wdrażania w organizacja ochrony danych osobowych. Na tym tle rozważa się perspektywy rozwoju i możliwości interpretowania i analizy RODO.

Słowa kluczowe: *administrator, bezpieczeństwo, dane osobowe, RODO, Rozporządzenie, UE*

General regulation on the protection of personal data (GDPR) – new challenges in the protection of personal data

Abstrakt

The aim of this study is to present and discuss the General Regulation on Data Protection – that is, GDPR is to standardize the level of data protection and provide a sense of legal certainty in the processing of personal data in all European Union countries. GDPR also imposes new obligations on entrepreneurs and government administration. Due to severe administrative penalties for non-compliance with GDPR provisions, it is worth already preparing for upcoming regulations. Methodological research appears both in connection with the introduction of the Regulation and the implementation process in the organization of personal data protection.

Keywords: *Administrator, security, personal data, GDPR, Regulation, UE*

ISSN: 1898-4509 e-ISSN: 2449-7436 online pdf

E-mail contact to the Author: jacek.bajorek@izbi.pl

Wprowadzenie

25 maja 2018 roku wchodzi w życie Rozporządzenie ogólne o ochronie danych osobowych (RODO), czyli unijne rozporządzenie dotyczące ochrony danych osobowych[1]. Nowe przepisy dotyczą każdego podmiotu funkcjonującego na obszarze UE, począwszy od jednoosobowych działalności gospodarczych, po duże międzynarodowe korporacje. Rozporządzenie wiązać będzie wszystkich, którzy przetwarzają dane osobowe w związku z prowadzoną działalnością gospodarczą. Wprowadza szereg zmian oraz rozszerza zakres obowiązków administratorów oraz podmiotów przetwarzających dane. Celem nowych przepisów jest również wyposażenie osób fizycznych oraz organów nadzorujących w skuteczne narzędzia reagowania na naruszenia Rozporządzenia.

Administratorzy danych będą zobligowani do realizowania nowych obowiązków, a właścicielom danych nadane zostaną dodatkowe uprawnienia. W efekcie powstanie konieczność wprowadzenia szeregu modyfikacji zarówno w obszarze organizacyjnym, jak i technicznym, czego skutkiem będzie m.in. konieczność dostosowania eksploatowanych dotychczas systemów teleinformatycznych.

Dokonując krótkiej charakterystyki wskazanej dyrektywy 95/46/WE, w pierwszej kolejności należy wskazać, że bez wątpienia celem jej wydania było pogodzenie interesów podmiotów informacji oraz interesów administratorów wykorzystujących dane osobowe w swojej działalności (Barta, Fajgielski, Markiewicz 2015, s. 34). Znajduje ona zastosowanie do wszelkich operacji lub zestawu operacji dokonywanych na danych osobowych, określanych jako przetwarzanie danych. Dyrektywa dotyczy danych przetwarzanych automatycznie oraz będących częścią lub mających być częścią nieautomatycznych zbiorów danych, w których informacje dostępne są na podstawie określonych kryteriów.

Nowe obowiązki administratora danych osobowych

Odwołując się do terminologii wprowadzonej przez art. 2 dyrektywy, dane osobowe powinny być rozumiane jako informacje dotyczące zidentyfikowanej lub możliwej do

[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. UE L 119/1, https://giodo.gov.pl/pl/569/9276.

zidentyfikowania osoby fizycznej. Dyrektywa konstytuuje obowiązek notyfikacyjny względem podmiotów danych, polegający na konieczności poinformowania ich o fakcie przetwarzania danych. Każdej z osób, której dane osobowe dotyczą, przyznane zostało również prawo dostępu do ich treści i sprzeciwu przed ich przetwarzaniem (o ile to możliwe, a przetwarzanie danych nie jest wymuszone np. przepisami prawa). Ustawodawca unijny zdecydował się również na objęcie pewnych kategorii danych szczególną ochroną, z uwagi na ich wyjątkowy związek ze sferą intymności człowieka.

Do kategorii tych należą dane dotyczące pochodzenia etnicznego lub rasowego, poglądów politycznych, przekonań religijnych, członkostwa w związkach zawodowych oraz informacje o szeroko rozumianym stanie zdrowia i życiu seksualnym. Dyrektywa zobowiązuje również administratorów danych do przedsięwzięcia odpowiednich technicznych oraz organizacyjnych środków ochrony przetwarzanych przez nich danych osobowych. Dyrektywa konstruuje również zasady przetwarzania danych, w tym najważniejszą zasadę legalności oraz celowości przetwarzania danych. Bezpośrednie stosowanie przepisów RODO (Kołodziej 2017, cz. II, s. 7).

Jednym z istotnych założeń RODO było ujednolicenie rozwiązań prawnych w zakresie ochrony danych osobowych w całej UE. Temu służy sam instrument w postaci rozporządzenia, a nie dyrektywy (która wymaga implementacji). Rozporządzenie unijne, jako akt prawa stosowany wprost i bezpośrednio, oznacza, że na jego podstawie mogą być podejmowane bezpośrednio rozstrzygnięcia, a także, że nie wymaga ono uchwalenia przepisów transponujących założenia rozporządzenia. Jedynie w sytuacji, w której ustawodawca w samym rozporządzeniu dopuścił taką możliwość, państwa członkowskie mają możliwość manewru.

W przypadku RODO jest co najmniej kilkanaście przepisów, które mogą zostać doprecyzowane lub odmiennie uregulowane przez poszczególne porządki prawne państw członkowskich (Barta, Litwiński 2015, s. 249). Wystarczy tutaj wymienić m.in. art. 8 RODO dotyczący dzieci i granicy wieku, który mówi, że państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową (w RODO 16 lat), która musi wynosić co najmniej 13 lat. We wspomnianym wyżej projekcie polskiej ustawy o ochronie danych osobowych zaproponowano właśnie obniżenie granicy tego wieku do lat 13.

Zmiany wprowadzone przez RODO

Zakres i skala zmian wprowadzonych do europejskiego porządku prawnego jest tak duża, że częściej o RODO mówi się jako o rewolucji, niż ewolucji. W dalszej części omówiono wybrane zmiany, które z perspektywy działalności administratorów oraz procesów mogą mieć największe znaczenie praktyczne.

W preambule RODO podkreślono, iż osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Przy odbieraniu zgód na przetwarzanie danych osobowych administrator musi pamiętać o spełnieniu tzw. obowiązku informacyjnego względem osoby, której dane dotyczą (Krzysztofek 2015, s. 76-77).

Najczęściej administratorzy, tworząc formularze zgód na przetwarzanie danych osobowych, umieszczają oświadczenie danej osoby wskazujące na to, iż została poinformowana o prawach jej przysługujących, bądź zamieszczają sformułowanie, z którego wynika, że administrator informuje o tych prawach. Do tej pory wiele organizacji narzekało na to, iż przez obowiązek informacyjny formularze zgód urastają do niebotycznych rozmiarów. Często prowadzi to również do trudności w pozyskiwaniu zgód na przetwarzanie danych osobowych od osób, których dane dotyczą, zniechęconych długością informacji, z którymi muszą się zapoznać.

Niestety, nowe przepisy nie ułatwiają wypełniania powyższego obowiązku administratorom danych. Zakres informacji, które muszą zostać zakomunikowane podmiotowi danych, zwiększył się trzykrotnie. Ogólne rozporządzenie o ochronie danych wymaga, aby wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Informacje o przetwarzaniu danych osobowych dotyczących osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli dane uzyskuje się z innego źródła – w rozsądnym terminie, zależnie od okoliczności, przy czym nie później niż w ciągu miesiąca po uzyskaniu danych.

Obowiązek informacyjny (Barta, Fajgielski, Markiewicz 2015, s. 498), unormowany w Ustawie o ochronie danych osobowych, przewidywał podanie następujących informacji

w sytuacji zbierania danych od osoby, której dane dotyczą: nazwę administratora i jego dane kontaktowe, cele przetwarzania danych, informacje o odbiorcach danych osobowych lub kategoriach odbiorców, informacje o prawach podmiotu danych (tj. prawie dostępu do danych, prawie ich poprawiania, dobrowolności podania danych lub obowiązku ich podania (Dmochowska, Zadrożny 2017, s. 16).

Rozszerzony obowiązek informacyjny administratora danych

W przepisach RODO istniejących dotychczas obowiązek informacyjny, nałożony na administratorów danych, został rozszerzony. Pod rządami RODO, każdy administrator danych będzie zobowiązany do informowania osoby, której dane dotyczą, o swojej tożsamość i danych kontaktowych, a jeżeli ma to zastosowanie o danych kontaktowych inspektora ochrony danych (Barta, Fajgielski, Markiewicz 2015, s. 584). Ponadto administrator danych jest zobowiązany także do podania: celu przetwarzania danych osobowych, podstawie prawnej przetwarzania oraz okresie, przez który dane osobowe będą przechowywane.

Administrator danych jest także zobowiązany do poinformowania osób, których dane dotyczą, o szeregu przysługujących im praw. Konieczne jest powiadomienie o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, a jeżeli przetwarzanie odbywa się na podstawie udzielonej zgody, także informacje o prawie do cofnięcia zgody. Ponadto osobę, której dane dotyczą, należy poinformować o prawie wniesienia skargi do organu nadzorczego oraz o profilowaniu.

Co do zasady każdy administrator danych będzie miał obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych. W rejestrze tym zamieszcza się m. in. następujące informacje: imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów (Gajda 2014, s. 57-58), a także gdy ma to zastosowanie – przedstawiciela administratora i inspektora ochrony danych, cele przetwarzania, opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych.

Kolejny obowiązkiem administratorów danych, który wprowadza RODO, jest przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Co jednak istotne, nie wszyscy administratorzy danych będą zobowiązani

do przeprowadzania takiej oceny. Zgodnie z przepisami RODO jest ona wymagana, jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli zatem planuje się uruchomienie nowego projektu, który będzie się wiązał z przetwarzaniem danych osobowych, to należy rozstrzygnąć, czy istnieje obowiązek przeprowadzenia oceny skutków dla ochrony danych osobowych.

Zapewnienie bezpieczeństwa przetwarzania danych osobowych jest najważniejszym i podstawowym obowiązkiem każdego administratora danych. Punkt ten jednak znalazł się na końcu mojego wpisu, ponieważ w miarę wydawania kolejnych wytycznych przez GIODO (Krzysztofek 2015, s. 57), planuje ten temat rozwinąć w kolejnych wpisach. Omawiając jednak w skrócie ten punkt trzeba wskazać, że w przeciwieństwie do obecnie obowiązujących przepisów, RODO nie wymaga prowadzenia dokumentacji bezpieczeństwa danych osobowych tj. Polityki bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym. Jednakże zgodnie z RODO, administrator wdraża odpowiednie środki techniczne i organizacyjne, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, tak aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać.

W praktyce oznacza to, że pomimo braku obowiązku prowadzenia dokumentacji ochrony danych osobowych, należy rozważyć, czy nie wdrożyć takiej dokumentacji w firmie. Przepisy RODO zobowiązują bowiem do wykazania, że dane osobowe w firmie są prawidłowo chronione, a jednym ze sposobów potwierdzenia spełnienia wymogów RODO, jest właśnie wprowadzenie odpowiedniej dokumentacji bezpieczeństwa danych osobowych (Barta, Fajgielski, Markiewicz 2015, s. 324).

Ocena skutków dla ochrony danych (DPIA)

Ocena skutków dla ochrony danych (ang. – *data privacy impact assessment*, DPIA; Konarski, Sibiga 2004, s. 551) to w pewnym sensie spojrzenie na proces przetwarzania danych osobowych oczami klienta. Wykonuje się ją wówczas, gdy przetwarzanie „z dużym

prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (Sierpień 2018) lub gdy operacje znajdują się w wykazie rodzajów operacji podlegających wymogowi dokonania tej oceny.

Motywy 89 i 90 rozporządzenia wyjaśniają, że ocena skutków jest jednym z mechanizmów, który pozwala na wyeliminowanie „ogólnego obowiązku zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych" (Kepa 2017) realizowanego kiedyś w postaci rejestracji zbiorów danych osobowych. Rozporządzenie eliminuje ten obowiązek, w którym administrator zgłaszał, zaś GIODO dokonywał oceny, czy przetwarzanie jest zgodne z prawem, czy zabezpieczenia są odpowiednie i czy przetwarzanie nie narusza niczyich praw i wolności.

Można założyć, że w organizacji powinno być mniej więcej tyle ocen skutków, ile kiedyś było zarejestrowanych zbiorów danych osobowych, pamiętając, że jako zbiór rozumiało się nie system komputerowy czy bazę, ale całokształt, czy też system gromadzenia i przetwarzania danych objęty tym samym celem. Na podobieństwa do zbiorów danych wskazuje też konieczność przeprowadzenia oceny „przed rozpoczęciem przetwarzania" – dokładnie tak samo był w przypadku zbiorów, przetwarzanie można było rozpocząć po wysłaniu zgłoszenia (Barta, Litwiński 2015, s. 243).

Jak się dobrze zastanowić, to zgłoszenie zbioru do rejestracji stanowiło prymitywną mieszankę rejestru czynności przetwarzania i oceny skutków. Należy wykonać DPIA dla każdego celu przetwarzania opisanego w rejestrze czynności przetwarzania (art. 30 ust. 1 Rozporządzenia o ochronie danych osobowych), o ile ten cel czy też operacje z nim związane powoduje konieczność wykonania DPIA.

W razie potrzeby, a przynajmniej, gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Jeśli do przetwarzania wykorzystuje się systemy informatyczne i coś się w nich zmienia, to będzie konieczność przeglądu (aktualizacji) dokonanych uprzednio ocen. Przykładowo migracja aplikacji do chmury bez wątpienia „wyzwoli" przegląd wszystkich DPIA wykonanych dla procesów przetwarzania, w których ta aplikacja bierze udział (Konarski, Sibiga 2004, s. 442-443).

Rozważmy przypadek, w którym organizacja będzie rozważać outsourcing zarządzania systemami do państwa trzeciego – w takiej sytuacji należy przeanalizować wszystkie

wykonane wcześniej DPIA. Właściwie to należałoby przyjrzeć się także i tym operacjom, które nie podlegały wcześniej DPIA, gdyż przez taką zmianę może się okazać, że pojawi się duże prawdopodobieństwo wysokiego ryzyka. Dlatego pewnie może okazać się, że najbezpieczniej będzie dokonywać oceny skutków dla ochrony danych osobowych dla każdego celu przetwarzania (Barta, Fajgielski, Markiewicz 2015, s. 509).

Prywatność na etapie projektu *privacy by design* i ustawienia domyślne *privacy by default*

Bezpieczeństwo i prywatność musi być wkomponowane w proces przetwarzania już na etapie projektowania rozwiązania. Przetwarzanie danych będzie wymagało przygotowania tzw. oceny skutków dla ochrony danych.

Podobnie ma się rzecz z *privacy by default* (można to tłumaczyć jako domyślna ochrona, chociaż nie za bardzo oddaje to istotę rzeczy). Wydaje się, że dla większych organizacji tego rodzaju wymogi stawiane przez rozporządzenie nie powinny stanowić problemu. Zatrudniają one obecnie ekspertów i/lub analityków bezpieczeństwa, którzy zapewniają, że ochrona jest wkomponowana w każde rozwiązanie (przykładowo patrz: Bygave 2014, s. 61).

Privacy by design i *privacy by default* powinno cieszyć wszystkich, bo zmniejszy samowolkę w rozmaitych rozwiązaniach, a przynajmniej tam, gdzie może to wpłynąć na prywatność. Pośrednio zmniejszy w ten sposób nieuczciwą konkurencję, która dzisiaj dostarcza tańsze rozwiązania kosztem bezpieczeństwa i prywatności.

Warto jeszcze wspomnieć o wykorzystywaniu wyłącznie danych niezbędnych do funkcjonowania danego rozwiązania. Przykładem tego może być ograniczona do kilku miesięcy historia operacji na rachunku dostępna w systemach bankowości elektronicznej. Użycie wyrazu „niezbędny" nie oznacza, że można zbierać tylko niezbędne dane osobowe, chodzi raczej o to, aby w określonych aplikacjach nie przechowywać więcej danych, niż potrzeba. Dotyczyć to będzie głównie aplikacji online i głównie tych udostępnianych klientom (Korga 2017, s. 202).

Na etapie projektowania rozwiązania trzeba będzie decydować się, jakie rozwiązania potrzebne będą do zabezpieczenia danych – istnieje tu oczywiście cała gama zabezpieczeń (w szczególności szyfrowanie transmisji danych czy danych w stanie spoczynku). Nie sposób nie wspomnieć o takich mechanizmach jak pseudonimizacja i anonimizacja.

Pseudonimizacja jest ciekawą i wygodną formą ograniczenia ryzyka, warto ją stosować, bo w razie wycieku danych osoba nieuprawniona nie będzie mogła z nich skorzystać, nie wiedząc, co te dane znaczą. Spotykana jest często w systemach oprogramowania szkół i uczelni, gdzie publikuje się wyniki egzaminów w postaci pseudoanonimowej. Dzięki rozporządzeniu będzie stosowane częściej.

Stosując pseudonimizację najlepiej używać nadanego przez organizację unikalnego numeru klienta, pracownika, agenta czy też numeru umowy. Numeru PESEL lub numeru dokumentu tożsamości lepiej nie używać – jest on przecież daną osobową.

To wszystko oznacza, że trzeba będzie doinwestować zespoły projektantów, upewnić się że rozumieją i znają się na bezpieczeństwie i ochronie danych osobowych i że wiedzą, jakie mechanizmy stosować, aby spełniać wymagania rozporządzenia.

Prawo do bycia zapomnianym

Jedną z istotniejszych zmian, jakie wprowadzi RODO, jest prawo do bycia zapomnianym, czyli ostatecznego i nieodwołalnego usunięcia danych osobowych z baz danych na żądanie zainteresowanego. Obecnie prawo do bycia zapomnianym dotyczy w zasadzie wyłącznie wyszukiwarek internetowych i nie opiera się na powszechnie obowiązujących przepisach, a na wyroku Trybunału Sprawiedliwości Unii Europejskiej.

Generalny Inspektor Danych Osobowych tłumaczy, że z prawa do bycia zapomnianym skorzystamy w sytuacji, w której chcemy, by nasze dane nie były przetwarzane, a na przykład określona instytucja czy firma nie mają podstawy do takiego przetwarzania. Jak zauważa Komisja Europejska, ten instrument ma zabezpieczać prywatność i dane osób, niekoniecznie usunięcie informacji z przeszłości albo ograniczanie wolności prasy.

To administratorzy danych osobowych, którymi są na przykład firmy, muszą przygotować bazy danych do przepisów RODO. Muszą m.in. sprawdzić dotychczasowe rozwiązania z zakresu ochrony danych osobowych i w wielu przypadkach je zmodyfikować. „W tym przypadku konieczne jest przeszukanie wszystkich zasobów teleinformatycznych, co będzie nie lada wyzwaniem, gdyż dane mogą być nie tylko w bazach, ale również w plikach tekstowych zlokalizowanych na komputerach użytkowników, plikach ze skanami dokumentów" (MS, ps/ms (2018).

Obowiązki inspektora ochrony danych (IDO)

Obowiązki inspektora ochrony danych w rozporządzeniu o ochronie danych zostały sformułowane w sposób ogólnikowy, bez wskazania trybu oraz terminów ich realizacji. Jest to istotna różnica w stosunku do tego, co obecnie przewiduje ustawa o ochronie danych osobowych i akty do niej wykonawcze w zakresie zadań administratora bezpieczeństwa informacji, zwanego dalej ABI (Barta, Litwiński 2016, s. 213).

Taki sposób ujęcia obowiązków inspektora jest wyrazem nowego podejścia do ochrony danych osobowych opartego na analizie ryzyka i zasadzie rozliczalności, zapisanej w art. 5 ust. 2 RODO. Wyznaczenie inspektorowi ochrony danych roli doradczej i weryfikacyjnej wobec działań administratora danych i podmiotu przetwarzającego (oraz ich pracowników) sprawia, że zarówno zadania IDO (Sakowska-Baryła 2017, s. 10-13), jak i sposób ich realizacji są ściśle powiązane nie tylko z obowiązkami administratorów danych lub podmiotów przetwarzających, ale też z nowym podejście do ich realizacji.

Przepis dotyczący zadań inspektora ochrony danych wskazuje na konieczność dostosowania trybu i metod pracy do specyfiki przetwarzania danych oraz związanego z nim ryzyka. Inspektor ma wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Chodzi tu o ogólną, zdroworozsądkową zasadę, którą IDO może odnieść do wielu aspektów swojej codziennej pracy. Wypełnianie zadań z należytym uwzględnieniem ryzyka wymaga od IDO ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko.

Zadania inspektora ochrony danych obejmować będą:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.
2. Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, w szczególności z użyciem nowych technologii, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogłyby powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Artykuł ten 39 ust 2 RODO nakłada obowiązek na administratora konsultowania się przy dokonywaniu oceny z inspektorem ochrony danych, jeżeli został on wyznaczony. Inspektor ochrony danych przedstawienia administratorowi opinii zakresie ochrony danych oraz monitorowania wykonania zaleceń wnikających z RODO (Gajda 2014, s. 89). IOD określa, kiedy i jak należy dokonywać oceny skutków dla ochrony danych, natomiast Administrator Danych decyduje w jaki sposób dokona oceny i wdroży zalecenia.
4. Obowiązek współpracy z organem nadzorczym oraz wypełniania przez organ nadzorczy zadań na rzecz m.in. inspektora ochrony danych. Wprowadzono to celu skonsolidowania bardziej efektywnego systemu monitorowania zgodności przetwarzania danych z RODO (Konarski, Sibiga 2004, s. 256-258).
5. Pełnienie funkcji osoby kontaktowej dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, a także w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
6. Pełnienie roli osoby kontaktowej dla tych, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
7. Obowiązek prowadzenia wewnętrznego rejestru czynności przetwarzania danych osobowych, za które odpowiada administrator danych, oraz rejestru kategorii czynności przetwarzania danych dokonywanych w imieniu administratora. Obejmuje to zarówno administratora, jak i podmiot przetwarzający dane osobowe.

Kary za brak wdrożenia RODO

Wraz z początkiem obowiązywania nowych przepisów dotyczących ochrony danych osobowych, czyli od 25 maja 2018 roku, można spodziewać się wzmożonej aktywności

organu nadzorczego, który będzie weryfikował stopień implementacji nowych regulacji w przedsiębiorstwie oraz wypełnienia obowiązków dotyczących przetwarzania danych osobowych.

Potencjalne stwierdzone braki oraz nieprawidłowości w zakresie przetwarzania danych osobowych mogą skutkować bardzo poważnymi konsekwencjami dla przedsiębiorców, począwszy od administracyjnych kar pieniężnych w wysokości nawet do 20 milinów euro, poprzez odpowiedzialność cywilną administratorów, a skończywszy nawet na odpowiedzialności karnej (Gutwirth, Leenes, de Hert 2016, s. 134).

Rozporządzenie wprowadza stosowne procedury kontrolne oraz kary za stwierdzone naruszenia w zakresie przetwarzania danych osobowych, pozostawiając przy tym jednocześnie państwom członkowskim pewną swobodę w tym zakresie poprzez możliwość przyjęcia odpowiednich przepisów krajowych.

Tabela 1. Kary finansowe związane z wejściem w życie przepisów RODO

Artykuł RODO	Kara finansowa
Art. 25. Naruszenie zasad ochrony danych osobowych w fazie projektowania (*privacy by design*), domyślna ochrona danych (*privacy by default*)	10 milionów euro lub do 2% wartości rocznego obrotu przedsiębiorstwa
Art. 29. Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego	10 milionów euro lub do 2% wartości rocznego obrotu przedsiębiorstwa
Art. 30. Rejestrowanie czynności przetwarzania	10 milionów euro lub do 2% wartości rocznego obrotu przedsiębiorstwa
Art. 31. Współpraca z organem nadzorczym	10 milionów euro lub do 2% wartości rocznego obrotu przedsiębiorstwa
Art. 32. Bezpieczeństwo przetwarzania	10 milionów euro lub do 2% wartości rocznego obrotu przedsiębiorstwa
Art. 5. Naruszenie zasad dotyczących przetwarzania danych osobowych	20 milionów euro lub do 4% wartości rocznego obrotu przedsiębiorstwa
Art. 7. Naruszenie warunków wyrażenia zgody na przetwarzanie danych	20 milionów euro lub do 4% wartości rocznego obrotu przedsiębiorstwa
Art. 15. Naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą	20 milionów euro lub do 4% wartości rocznego obrotu przedsiębiorstwa
Art. 16. Naruszenie wykonania prawa do sprostowania i usuwania danych	20 milionów euro lub do 4% wartości rocznego obrotu przedsiębiorstwa

Źródło: opracowanie własne.

Z powyższej możliwości skorzystał polski ustawodawca przygotowując nowy projekt ustawy o ochronie danych osobowych. Rozszerza on określoną w RODO odpowiedzialność podmiotów przetwarzających dane osobowe oraz katalogi sankcji m.in. o odpowiedzialność karną (choć równocześnie nowy projekt ogranicza odpowiedzialność karną w stosunku do tej, która obowiązuje na gruncie aktualnej ustawy o ochronie danych osobowych).

Wysokość kar wskazanych w rozporządzeniu zostanie dopasowana do polskich realiów, jednak w kwestii przystosowania przepisów krajowych do regulacji ogólnego rozporządzenia o ochronie danych osobowych istnieje jeszcze wiele niewiadomych. Z pewnością wraz ze zbliżaniem się tak ważnej dla ochrony danych osobowych daty – 25 maja 2018 roku – będziemy wiedzieć coraz więcej.

Podsumowanie

Rozporządzenie spowoduje, że zasady prywatności i ochrony danych staną się wizytówką Unii Europejskiej i zaczną przenikać też do innych państw, proces ten już się dzieje. Tym, co je wyróżnia, jest kontekst państwowy, związany z kwestiami kultury i mentalności prywatności i ochrony danych. Powstaje zatem szereg pytań oto, na ile polskie RODO wykorzystuje szanse, by te nowe zasady wywarły pozytywne zmiany i dążenie do wysokich standardów.

W trosce o realizację podstawowego prawa obywateli do prywatności i ochrony ich danych osobowych, unijny ustawodawca stworzył ogólne rozporządzenie o ochronie danych. Aby zapewnić funkcjonowanie tych nowych regulacji, przewidział możliwość nakładania wysokich kar finansowych. Jak to często bywa, gdy ktoś zyskuje, to ktoś inny traci. To, co dla obywateli jest uprawnieniem, dla przedsiębiorców staje się obowiązkiem i kosztem. Działania dostosowawcze, szczególnie w dużych organizacjach, mogą okazać się kosztowne. Można założyć, że dla wielu z nich będą to wydatki nieprzewidywalne do tej pory w budżecie. Ustawodawca, mając tego świadomość, dał wszystkim krajom członkowskim Unii Europejskiej dwa lata okresu dostosowawczego. Czas ten mija 25 maja 2018 roku.

Mimo, że przedsiębiorcy patrzą na nowe regulacje często przez pryzmat zbędnej biurokracji generującej dodatkowe koszty, należy zauważyć, że dostosowanie się do nich szczególnie w długoterminowym okresie okaże się dla nich korzystne. Dzięki nowym

przepisom, w tym realnej groźbie dotkliwej kary finansowej, zostaną zmuszeni do systemowej, przemyślanej i skutecznej ochrony tego, co dla wielu organizacji jest najcenniejsze, a mianowicie do ochrony informacji. Chroniąc dane osobowe niejako samoistnie rozciągnięty zostanie parasol ochronny na inne informacje, stanowiące np. tajemnicę finansową, technologiczną czy know-how przedsiębiorstwa.

Bibliografia

Barta J., Fajgielski P., Markiewicz R. (2015), *Ochrona danych osobowych. Komentarz*, Warszawa: Wolters Kluwer S.A.

Barta P., Litwiński P. (2015), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: C.H. Beck

Bielak-Jomaa E. (2016), *Polska i europejska reforma ochrony danych osobowych*, (w:) *Polska i europejska reforma ochrony danych osobowych*, (red.) E. Bielak-Jomaa, D. Lubosz, Warszawa: Wolters Kluwer S.A.

Bygrave L.A. (2014), *Data Privacy Law. An International Perspective*, Oxford: Oxford University Press

Dmochowska A., Zadrożny M. (2017), *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa: C.H. Beck

Gajda A., (2014), *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace/ Szkoła Główna Handlowa" nr 4

Gutwirth S., Leenes R., De Hert P. (2016), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Brussels: Springer Netherlands

Kepa L. (2017), *Jak rozporządzenie unijne wpłynie na funkcjonowanie IT*, https://superabi.pl/artykul/jak-rozporzadzenie-unijne-RODO-wplynie-na-funkcjonowanie-IT

Konarski X., Sibiga G. (2004), *Zmiany w ustawie o ochronie* danych osobowych w świetle Dyrektywy 95/46/WE, „Monitor Prawniczy" nr 12

Kołodziej M. (2017), *Vademecum ABI. Część II Przygotowanie do roli Inspektora Ochrony Danych*, Warszawa: C.H. Beck

Korga M. (2017), *Przygotowanie organizacji do stosowania RODO.* Ochrona danych w okresie przejściowym i po wejściu przepisów w życie, Warszawa: Presscom

Krzysztofek M. (2015), *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, Warszawa: Wolters Kluwer S.A.

MS, ps/ms (2018), *Prawo do usunięcia z internetu danych. Za złamanie tych zasad będą potężne kary*, https://tvn24bis.pl/z-kraju,74/rodo-zmiany-w-ochronie-danych-osobowych-w-2018-r,801917.html

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. UE L 119/1, https://giodo.gov.pl/pl/569/9276

Sakowska-Baryła M. (2017), *Obowiązek wyznaczenia IOD w podmiotach publicznych*, (w:) ABI Expert, http://www.abi-expert.pl/wydania/kwiecien-czerwiec-2017/art,1658,obowiazek-wyznaczenia-iod-w-podmiotach-publicznych.html

Sierpień M. (2018), *Przetwarzasz dane na dużą skalę? Sprawdź, jakie będziesz miał obowiązki według RODO,* https://www.poradyodo.pl/odpowiedzialnosc-abiado/przetwarzasz-dane-na-duza-skale-sprawdz-jakie-bedziesz-mial-obowiazki-wedlug-rodo-8452.html