OCHRONA DANYCH OSOBOWYCH W PRZEDSIĘBIORSTWIE

Janusz RYBIŃSKI

Wojskowa Akademia Techniczna

Abstrakt. Obowiązujący w naszym kraju system prawny chroni dane osobowe wszystkich mieszkańców Polski. System ten wykształcił się wraz ze zmianami ustrojowymi w latach 90. ubiegłego wieku. Przez czas jego stosowania był nowelizowany pod kątem stworzenia bardziej skutecznego i efektywnego sposobu chroniącego dobro wszystkich ludzi. Tworzenie prawa to zadanie Sejmu i Senatu, jednak jako członek Unii Europejskiej jesteśmy również zobowiązani stosować prawo unijne. W tym zakresie działalność legislacyjna jest stosunkowo dynamiczna, ponieważ od wielu lat dąży się do wprowadzenia w całej Unii Europejskiej jednakowych standardów ochrony. Te standardy wchodzą w życie już w maju 2018 r. i faktycznie zmieniają wiele regulacji w obowiązujących zasadach ochrony. Celem artykułu jest przedstawienie dotychczasowych zasad ochrony oraz omówienie najważniejszych regulacji wprowadzonych przez prawo unijne i skutków ich stosowania tam, gdzie będą one najbardziej widoczne, czyli w polskich przedsiębiorstwach.
Słowa kluczowe: dane osobowe, ochrona danych osobowych.

Wstęp

We współczesnym świecie działalność gospodarcza jest regulowana wieloma przepisami prawa, jednym z nich jest ustawa o ochronie danych osobowych. Regulacje odnoszące się do ochrony danych osobowych dotyczą nie tylko przedsiębiorstw, ale praktycznie każdego obywatela. W artykule skupiono się jednak na problematyce przedsiębiorstwa, ponieważ odgrywa ono szczególną rolę w życiu społeczeństwa. Drugi powód dotyczy faktu, że w zakresie ochrony danych osobowych w przedsiębiorstwie mają zastosowanie prawie wszystkie jego przepisy ustawowe, także te wynikające z aktów wykonawczych w postaci rozporządzeń ministerialnych. Należy też pamiętać, że przepisy prawa zawsze traktują obszar regulacji stosunkowo szeroko, definiując pojęcia, regulując i porządkując wiele obszarów i sytuacji, które mogą występować, ale nie muszą. W przypadku działalności gospodarczej pracodawca musi spełnić wiele różnych warunków, ponieważ ten zakres ochrony dotyczy każdego pracownika przedsiębiorstwa, niezależnie od jego stanowiska, a jeżeli jest to przedsiębiorstwo usługowe, będzie to dotyczyło również wszystkich klientów i dostawców związanych z tym przedsiębiorcą.

Dane osobowe znalazły się w systemie ochrony prawnej, który wykształcił się pod koniec lat 90. ubiegłego wieku, wraz ze zmianami ustrojowymi w państwie. Podstawowe regulacje to ustawa dotycząca ochrony danych osobowych i akty wykonawcze, które precyzowały kwestie wynikające z ustawy. Nadrzędnym aktem prawnym jest oczywiście Konstytucja RP, która gwarantuje każdemu obywatelowi prawo do prywatności oraz

do ochrony dotyczących go danych. Prawo krajowe było wielokrotnie nowelizowane, aby stworzyć bardziej skuteczny system ochrony. Te zadania leżą w gestii Sejmu i Senatu, jednak Polska, jako członek Unii Europejskiej, jest również zobowiązana do stosowania prawa unijnego, w którym wielokrotnie nowelizowano zasady tej ochrony.

Polskie prawo z tego zakresu datuje swój początek na 1997 r. i zostało wprowadzone w postaci ustawy[1]. Regulowała ona wszystkie kwestie związane z ochroną danych osobowych, w tym przykładowo prawa osób fizycznych i obowiązki instytucji, które dysponowały tego rodzaju danymi. Wpływ na treść tych regulacji miały jednak przepisy międzynarodowe, a zwłaszcza Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu danych.

Problematyka wpływu prawa międzynarodowego na regulacje krajowe ma swój dalszy ciąg w postaci dążenia do wprowadzenia w całej Unii Europejskiej jednakowych standardów ochrony. Standardy te to RODO, weszły w życie w maju 2018 r. i faktycznie zmieniają wiele pojęć i regulacji w dotychczasowych zasadach ochrony. Samo ich przygotowanie trwało kilka lat, ponieważ już w 2016 r. podjęto decyzję o ich gruntownej nowelizacji, dając wszystkim podmiotom dwuletni okres na przygotowanie się do ich wprowadzenia. Głównym celem tych zmian jest wprowadzenie jednakowych zasad ochrony, zwiększenie praw osób, których dane dotyczą, oraz zaostrzenie kar za nieprzestrzeganie przepisów. Celem nadrzędnym nie jest zburzenie dotychczasowych regulacji i systemu ochrony prawnej, który został stworzony, lecz jedynie jego udoskonalenie i spowodowanie, że stanie się on skuteczniejszym narzędziem ochrony, jednakowym na całym obszarze Unii Europejskiej, a tym samym zwiększającym zaufanie obywateli do wszystkich administratorów dysponujących naszymi danymi osobowymi.

System ochrony danych osobowych

Ustawa o ochronie danych osobowych z 1997 r. wprowadziła wiele regulacji, które miały chronić dane obywateli, a także dawały wszystkim szereg uprawnień[2]. Na podstawie ustawy wydano wiele aktów wykonawczych w postaci rozporządzeń

[1] W ciągu kilku lat od wejścia w życie ustawy ukazały się dwa komentarze i tak: A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999 r., J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wyd. Zakamycze, 2001 r.

[2] W zakresie ogólnym ustawa skonkretyzowała konstytucyjnie zagwarantowane prawo do decydowania o tym, komu, w jakim zakresie i w jakim celu przekazywane są dane osobowe; wyposażyła osoby, których dane są wykorzystywane, w środki służące do realizacji tego prawa, jak również powołała organ – Generalnego Inspektora Ochrony Danych Osobowych (GIODO) – który stoi na straży przysługującego każdemu prawa.

lub zarządzeń, porządkujących problematykę jedynie zasygnalizowaną w ustawie. Wszystkie te akty prawne łącznie tworzą system prawa, który w tym wypadku obejmuje zagadnienie ochrony danych osobowych w państwie. Na ten system prawny składają się również akty prawa międzynarodowego, ponieważ to zmiany konwencji, dyrektyw lub rozporządzeń stawały się podstawą nowelizacji przepisów krajowych. Z uwagi na bardzo częste i istotne zmiany w tym zakresie warto przedstawić podstawowe dokumenty prawa, które przez ponad 20 lat stanowiły podstawę ochrony danych osobowych w Polsce.

1. Podstawowym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia ochrony danych osobowych, była Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Sporządzona w Strasburgu (Dz.U. z 2003 r. Nr 3, poz. 25).
2. Istotnym aktem prawnym jest Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23 listopada 1995 r.).
3. W Polsce taką rolę pełni ustawa zasadnicza: Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483)[3].
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r., Nr 133, poz. 883 z późniejszymi zmianami)[4].
5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024).
6. Rozporządzenie MSWiA z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2004 r., Nr 94, poz. 923) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.
7. Rozporządzenie MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., Nr 229, poz. 1536) – wydane na podstawie art. 46a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia.

---

[3] W Konstytucji ochronę danych zawarto w art. 47 i art. 51.

[4] Art. 1. Ustawy stanowi: „Każdy ma prawo do ochrony dotyczących go danych osobowych" oraz „Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i w trybie określonym ustawą".

8. Dyrektywa 97/66WE Parlamentu Europejskiego i Rady z dnia 15.12.1997 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w dziedzinie telekomunikacji (Dz.Urz. WE L24 z 30 stycznia 1998 r.)[5].
9. Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (Dz.Urz. WEL 178 z 17 lipca 2000 r.).
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r., Nr 112, poz. 1198 z późniejszymi zmianami).
11. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r., Nr 144, poz. 1204 z późniejszymi zmianami).
12. Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. z 2010 r., Nr 229, poz. 1497), ustawa weszła w życie 7 marca 2011 r.
13. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r., Nr 159, poz. 948).
14. Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r., Nr 225, poz. 1350).
15. Ostatnie z nich to 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).

Przedstawiając tak obszerny system prawny i wiele regulacji, które dotyczą tej problematyki, zawsze rodzi się pytanie o jego zasadność. Odpowiedź na takie pytanie to często istota wszelkich działań. W tym wypadku mamy do czynienia z postępem gospodarczym i szybkim rozwojem nowych technologii, zwłaszcza informatycznych, stanowiących zagrożenie dla tego obszaru działalności człowieka, który można określić prywatnością. Łatwość, z jaką dane osobowe są gromadzone i przechowywane przez różne instytucje, sprawia, że jednostka nie jest w stanie kontrolować zarówno obiegu, jak i treści swoich danych osobowych. W związku z tym dostrzeżono konieczność objęcia tej sfery prywatności ochroną państwa[6].

[5] W nomenklaturze prawniczej akty prawne wymienione w poz. 8-14 regulują zasady ochrony danych osobowych, jednak zawierają przepisy szczególne.

[6] A. Kowalik (red.), *ABC ochrony danych osobowych*, Wyd. Sejmowe, Warszawa 2007 r., s. 5.

Taką rolę spełniała ustawa o ochronie danych osobowych z 1997 r. regulująca zasady ochrony danych, które faktycznie stanowią część poufnej wiedzy utajnionej[7]. Porządkuje ona więc całe spektrum zagadnień, począwszy od praw osób, których dotyczą, poprzez obowiązki podmiotów – administratorów zarządzających naszymi danymi osobowymi, po zasady ich przetwarzania, zabezpieczania oraz rejestrację zbiorów danych, zasady ich przekazywania za granicę i regulacje dotyczące nadzoru nad posiadanymi danymi osobowymi[8].

Geneza zmian prawa o ochronie danych osobowych

Problematyka ochrony danych osobowych, obecnie tak szeroko popularyzowana w mediach w związku z wejściem RODO, jeszcze w I połowie XIX wieku była właściwie nieznana[9]. Zainteresowanie nią to dopiero II połowa XIX wieku, kiedy pojawiają się pierwsze przepisy z tego zakresu, jednak brakuje jednolitego aktu prawnego, który regulowałby ten problem całościowo. W późniejszym okresie fragmentaryczne regulacje pojawiają się w dokumentach prawnych ONZ[10]. Kompleksowe ujęcie problematyki ochrony danych osobowych występuje w prawie Unii Europejskiej.

Cały proces legislacyjny z zakresu ochrony danych osobowych rozpoczął się od uchwalenia Dyrektywy 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu danych. Kolejnym krokiem było przyjęcie polskiej Ustawy o ochronie danych osobowych 29 sierpnia 1997 r. Propozycje kompleksowych zmian tego systemu w całej Unii Europejskiej zostały zainicjowane 4 listopada 2010 r., a 25 stycznia 2012 r. rozpoczęto nad nimi dyskusję. Chcąc dostosować się do tych przepisów i przygotowując grunt pod przepisy europejskie, w Polsce w dniu 7 listopada 2014 r. podjęto pracę nad ułatwieniami wykonywania działalności gospodarczej. Przepisy tej ustawy weszły w życie z dniem 1 stycznia roku następnego. Omawiane przepisy RODO uchwalono 26 kwietnia 2016 r. z terminem wejścia w życie z dniem 25 maja 2018 r.

---

7 Por. W. Kotarba, *Ochrona wiedzy w Polsce*, Wyd. Instytutu Organizacji i Zarządzania „Orgmasz", Warszawa 2005, s. 12.

8 J. Rybiński, *System zarządzania innowacjami w resorcie obrony narodowej*, Wyd. Wojskowa Akademia Techniczna, Warszawa 2007, s. 59.

9 RODO to powszechnie używany skrót Rozporządzenia o Ochronie Danych Osobowych.

10 Przykładem tego typu regulacji może być Rezolucja 45/95 Zgromadzenia Ogólnego ONZ z dnia 26 czerwca 1985 r., która zawiera wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych. Jak wszystkie tego typu dokumenty, nie posiadała charakteru wiążącego, a jedynie stanowiła zalecenia odnośnie do gwarancji, jakie powinny być zapewnione w przepisach krajowych.

RODO to Rozporządzenie o ochronie danych osobowych wydane przez Parlament Europejski i Radę UE w 2016 roku, a dotyczy ochrony danych osób fizycznych w zakresie przetwarzania danych osobowych. Weszło w życie 17 maja 2016 roku, natomiast w Polsce zaczęło obowiązywać od 25 maja 2018 roku. RODO dotyczy wszystkich podmiotów, które w związku z prowadzoną działalnością gospodarczą przetwarzają dane osobowe. W tej sytuacji przestanie obowiązywać Dyrektywa 95/46 WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych z 1995 roku. Z treści ww. przepisów wynika, że czas między uchwaleniem przepisów a ich wejściem w życie ma służyć głównie dostosowaniu przepisów krajowych, a także umożliwić administratorom danych przygotowanie się do realizacji nowych obowiązków, co zostało zawarte w preambule, która stanowi: „…przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów”[11].

Przedstawiając podstawowe regulacje RODO, należy zwrócić uwagę na zasadnicze zmiany, jakie wprowadza:

- RODO obowiązuje w Polsce od 25 maja 2018 r.;
- wprowadza wysokie kary za łamanie przepisów, zostało to określone w następujący sposób: 20 milionów euro lub 4% wartości rocznego obrotu;
- dla tych przepisów wprowadzono globalny zasięg, czyli obowiązują wszędzie tam, gdzie są przetwarzane dane osobowe obywateli Unii Europejskiej;
- przewidziano stosowne narzędzia celem uzyskania zgodności z RODO;
- wprowadzono obowiązek szybkiego zgłaszania wszelkich incydentów w tym zakresie, przewidując wysokie kary, jeżeli nie zostaną one zgłoszone w ciągu 72 godzin;
- rozszerzono prawa podmiotu danych o prawo do bycia zapomnianym oraz rozbudowano prawo do informacji[12].

Okres poprzedzający wprowadzenie tych przepisów to wiele różnego rodzaju publikacji, wyjaśnień i interpretacji przyszłego stanu prawnego. W celu wyjaśnień określono, że w praktyce stosowania przepisów będzie to oznaczało, że:

- Wprowadzono obowiązek zgłaszania naruszeń, ponieważ każdy administrator danych osobowych będzie musiał w ciągu 72 godzin zgłosić do odpowiedniego organu fakt naruszenia praw i swobód osób, których dane zostały naruszone. Kolejnym jego obowiązkiem wynikającym z tego zapisu będzie obowiązek poinformowania o fakcie naruszeń osoby, których te dane dotyczą.
- Ustanowiono odpowiedzialność przetwarzającego dane, ponieważ wszystkie podmioty przetwarzające dane osobowe pochodzące z innych firm będą

[11] Por. motyw 171 preambuły Rozporządzenia o ochronie danych osobowych.
[12] https://giodo.gov.pl/pl/p/informacje-ogolne (dostęp 20.05.2018 r.).

bezpośrednio odpowiadać za naruszenie zapisów zawartych w Rozporządzeniu o ochronie danych osobowych oraz podlegać karze finansowej, która maksymalnie może sięgać 20 mln euro. Kara ta została określona w maksymalnej wysokości i należy sądzić, że będzie nakładana proporcjonalnie do rodzaju przewinienia.

- Wprowadzono prawo obywateli do bycia „zapomnianym", ponieważ każdy w związku z zapisami RODO będzie miał prawo złożyć wniosek o zapomnienie danych, czyli w praktyce o usunięcie swoich danych z bazy danych. Jednocześnie każdy może domagać się przeniesienia swoich danych oraz pełnego do nich dostępu i wglądu.
- Wprowadzono wyznaczenie Inspektora Danych Osobowych, co będzie obowiązkiem niektórych firm kontrolujących lub przetwarzających dane osobowe. Osoba wyznaczona do pełnienia takich obowiązków powinna posiadać pełną wiedzę z zakresu przetwarzania i ochrony wrażliwych danych.
- W Rozporządzeniu zdefiniowano, czym konkretnie są dane wrażliwe, a także rozszerzono to pojęcie o dane genetyczne i biometryczne.
- Wprowadzono nowe pojęcie inwentaryzacji danych, ponieważ każdy administrator danych osobowych będzie zobowiązany do przygotowywania rejestrów, które będą musiały zawierać takie informacje jak: powód przetwarzania danych, rejestr naruszeń i incydentów, wykaz sposobów ochrony prywatności czy też wymóg gromadzenia zgód na przetwarzanie danych.
- Przyjęto nowe regulacje dotyczące profilowania. Regulacje wprowadzają ograniczenia w profilowaniu, tzn. dany podmiot będzie musiał uzyskać zgodę na profilowanie jeszcze przed rozpoczęciem zbierania danych. RODO nałożyło jednocześnie obowiązek informowania o profilowaniu osób, których będzie ono dotyczyć.

Rozporządzenie o ochronie danych osobowych wprowadza nowe zasady uzyskiwania zgody na przetwarzanie danych, a także przepisy dotyczące uzupełniania uzyskanej zgody, które już istnieją[13].

Przetwarzanie danych osobowych w przedsiębiorstwie na podstawie RODO

Przedsiębiorstwa, uwzględniając wytyczne RODO, szeroko informowały swoich pracowników i klientów o wprowadzonych zmianach, jakie nastąpiły w zakresie ochrony danych osobowych w maju 2018 r. Przygotowując zasady ochrony danych

[13] https://odo24.pl/blog-post.rodo-najwazniejsze-zmiany-i-nowosci-infografika (dostęp 1.08.2018 r.).

osobowych, uwzględniono wszystkie elementy, które tym zmianom uległy[14]. Najszerszy ich zakres zawierają regulaminy lub zasady, zmiany albo dostosowanie się do przepisów RODO, nazywane różnie w zależności od przedsiębiorstwa – firmy, jednak dotyczą tego samego. Aby je przybliżyć i omówić najważniejsze z nich, dokonano analizy zmian, które przygotowała dla swoich klientów sieć komórkowa Orange Polska SA[15].

W opracowaniu *RODO, czyli zmiany w przepisach dotyczących ochrony danych osobowych* zawarto podstawowe wyjaśnienia, które mają rozwiać wszelkie wątpliwości z tym związane. Po pierwsze, wyjaśniono, co to jest RODO, dalej, jaki jest jego cel, od kiedy obowiązuje i co zawarto w dokumencie. Ważną informacją jest to, że w związku z wejściem przepisów nie ma potrzeby kontaktowania się z Orange Polska SA. Wyjaśniając podstawowe kwestie, powtórzono za Rozporządzeniem ich znaczenie, podobnie jak i cel Rozporządzenia, którym jest ujednolicenie zasad przetwarzania danych osobowych na całym obszarze Unii Europejskiej[16].

W części zasadniczej dokument otwiera stwierdzenie, że Orange Polska SA w świetle przepisów jest **administratorem** danych osobowych klientów, co oznacza, że jest odpowiedzialne za bezpieczne i zgodne z prawem ich wykorzystanie.

Dane osobowe uzyskane w trakcie zawierania umowy oraz podczas jej trwania są wykorzystywane w celu:

- Zawarcia i wykonania umowy, w tym zapewnienia poprawności i jakości usług (usuwania awarii i sprawdzania poprawności działania usługi) – przez czas obowiązywania umowy i jej rozliczenia po zakończeniu.
- Wykonywania ciążących na Orange Polska SA obowiązków prawnych, w tym wystawianie faktur i dokumentów księgowych, udzielanie odpowiedzi na reklamacje oraz zapewnianie bezpieczeństwa sieci zgodnie z przepisami prawa telekomunikacyjnego. Zastrzeżono ponadto, że z danych osobowych Orange Polska SA będzie korzystać w celu realizacji obowiązków prawnych przez cały czas trwania umowy i przez czas, kiedy przepisy nakazują ich przechowywanie, np. kiedy firma może ponieść konsekwencje prawne niewykonania zobowiązania.
- Wykrywania nadużyć i zapobiegania im przez cały czas trwania umowy i przez okres, kiedy przedawniają się roszczenia wynikające z umowy.

---

[14] http://prawo.gazetaprawna.pl/artykuly/1084200,10-najwazniejszych-rzeczy-o-rodo-ktore-musisz-znac.html (dostęp 1.08.2018 r.).

[15] Orange Polska SA jest liderem na polskim rynku telefonii stacjonarnej, Internetu i transmisji danych. Jako jedyny operator oferuje kompleksowe rozwiązania telekomunikacyjne dostępne w całym kraju. http://www.orange.pl/orange_polska.phtml;osid=3D152E349831D18A37CDFB11C5C299FA.ocpwww806?_requestid=125211 (dostęp 2.08.2018 r.).

[16] http://www.outsourcingportal.eu/pl/3-najwazniejsze-korzysci-z-nowej-ustawy-o-rodo (dostęp 1.08.2018 r.).

- Ustalenia, obrony i dochodzenia roszczeń – podstawa prawna to uzasadniony interes prawny.
- Marketingu bezpośredniego – przez czas trwania umowy.
- Tworzenia zestawień analiz i statystyk na potrzeby wewnętrzne, raportowania, planowania usług i prac rozwojowych.
- Weryfikacji i wiarygodności płatniczej, przez okres niezbędny do dokonania takiej oceny, przy zawarciu, przedłużeniu lub rozszerzeniu zakresu umowy.
- Wsparcia obsługi, przykładowo informowanie o awariach, dostosowaniu usług do przedstawianych ofert czy też o złożonych reklamacjach.

Dokument uregulował również zakres danych, które wymagane są od klientów. Podzielono je na bezwzględne i względne. Zawierając umowę, należy podać imię, nazwisko, numer PESEL lub serię i numer dowodu potwierdzającego tożsamość. Ważny jest też numer telefonu lub adres mailowy w celu utrzymania kontaktu. Podawanie danych nie jest wymogiem ustawowym, jednak przepisy nakazują dokonanie rejestracji, która obejmuje ww. dane. Zawierając umowę, można upoważnić Orange Polska SA do weryfikacji wiarygodności płatniczej, zamówić dodatkowe usługi lub skorzystać z funkcjonalności nieobjętych dotąd umową. Te dane osobowe będą stanowiły dodatkowe informacje o danych klienta.

Stosunkowo szeroko uregulowano prawo do przekazywania danych. Dane klientów przekazywane są:

- Podmiotom przetwarzającym dane w imieniu Orange Polska SA, np. agentom, podwykonawcom, a także podmiotom utrzymującym sieć telekomunikacyjną.
- Innym administratorom. Wymienia się między innymi współpracujące agencje reklamowe, podmioty prowadzące działalność pocztową i kurierską, podmioty nabywające wierzytelności (po spełnieniu określonych warunków), Związek Banków Polskich oraz podmioty współpracujące przy obsłudze spraw księgowych[17].

Kolejne istotne informacje zostały zawarte w części dotyczącej danych z innych źródeł, gdzie wymieniono dwa przypadki tego typu. Po pierwsze, w posiadanie danych Orange Polska SA może wejść, jeżeli zostanie zawarta umowa na usługi NC+ i za świadczenie usługi nie zostanie dokonana opłata. W takim wypadku będzie przysługiwało prawo do dochodzenia roszczeń. Druga sytuacja dotyczy również opłat, konkretnie banku i numeru konta w przypadku dokonywania rozliczeń, np. zwrotu nadpłaty. Jednocześnie zamieszczono informacje, że operator nie planuje przekazania danych klientów poza Unię Europejską.

[17] W tym zakresie wymienia się dziewięć przypadków, lecz każdy z nich jest w stosowny sposób uzasadniony i w stosunku do każdego została podana podstawa prawna.

W zakresie automatycznego podejmowania decyzji wymieniono kilka przypadków, kiedy takie decyzje będą podjęte i mają istotny skutek dla klientów. Te sytuacje to głównie niewywiązywanie się z umów. Określono je w sposób następujący:

- przy zawieraniu umowy podejmowana jest automatyczna decyzja o ocenie wiarygodności płatniczej;
- w ramach warunków umowy, jeżeli systemy automatyczne odnotują osiągnięcie progu limitów;
- w celu wykrywania nadużyć przy korzystaniu z usług – aby reagować na określone nadużycia;
- w przypadku zalegania z opłatami.

Stosunkowo obszernie przedstawiono problematykę danych transmisyjnych o lokalizacji i dostępie do dekoderów. Tego typu dane są przetwarzane w celu:

- wykonania umowy, w tym realizacji połączeń, zapewnienia ich jakości wynikającej z umowy i naliczenia stosownych opłat, a także w celu rozpatrywania reklamacji;
- zarządzania ruchem w sieciach telekomunikacyjnych oraz rozliczeń z innymi operatorami;
- zapewnienia bezpieczeństwa sieci, a także wykrywania nadużyć i zapobiegania im;
- ustalenia faktów i obrony oraz dochodzenia roszczeń;
- przechowywania na potrzeby ewentualnych przyszłych postępowań;
- marketingu bezpośredniego pod warunkiem wyrażenia zgody.

Dane transmisyjne można wykorzystać lub przechowywać przez czas trwania umowy, a po jej zakończeniu przez czas dochodzenia roszczeń. Dane o lokalizacji również mogą być wykorzystywane, do celów przewidzianych stosownymi przepisami. W dokumencie uwzględniono możliwość opublikowania danych klientów w spisach abonentów i informacjach o numerach telefonów. Takie umieszczenie nazwisk i numerów telefonów zawsze będzie wymagało zgody[18].

Z pozostałych regulacji na uwagę zasługują uprawnienia klientów do sprostowania (poprawienia danych); usunięcia danych przetwarzanych; ograniczenia przetwarzania (stosownie do złożonego wniosku); dostępu do danych (można uzyskać informacje o przetwarzanych danych oraz kopię danych), a także przeniesienia danych do innego administratora[19]. Ponadto uregulowano prawo sprzeciwu, które jest niezależne od praw wcześniej wymienionych. Sprzeciw można wnieść wobec przetwarzania, w tym profilowania na potrzeby marketingu bezpośredniego. Jednocześnie w dowolnym momencie można wnieść sprzeciw w przypadkach określonych dla tego rodzaju działania.

---

[18] https://www.orange.pl/mojedane (dostęp 1.08.2018 r.).

[19] Por. art. 20, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W zakończeniu powyższych regulacji zawarto problematykę dotyczącą wyrażenia zgody związanej z realizacją umowy, ta zgoda również może w każdej chwili być wycofana i nie będzie to wpływać na zgodność z prawem wykorzystania danych przed jej cofnięciem. W przypadku gdy klient będzie miał poczucie, że przetwarzane dane osobowe naruszają przepisy prawa, może wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych[20].

Nowy stan prawny to również okazja do poszukiwania wiedzy na ten temat[21]. Dla każdego przedsiębiorstwa ważne jest, w jaki sposób stosować się do wymogów nowej ustawy; jak zabezpieczyć swoje dane według wymogów RODO; jak przygotować zgodę na przetwarzanie danych osobowych i co powinna zawierać; w jaki sposób zarejestrować zbiory danych; co grozi za nieprzestrzeganie przepisów o ochronie danych osobowych oraz jak przygotować się na wprowadzenie nowych przepisów. Ważne informacje z tego zakresu dotyczą tego, jak wygląda kontrola przestrzegania przepisów, a także jak postępować w przypadku wycieku danych osobowych[22].

Przedstawiona problematyka w teorii wydaje się obejmować całość problemów, jakie mogą wyniknąć w praktyce stosowania przepisów. Jednak życie zaskakuje i wyprzedza teorię niejednokrotnie w sposób trudny do przewidzenia. Wprowadzenie RODO spowodowało wiele absurdalnych sytuacji. Bez wizyty w urzędzie nie jesteśmy w stanie uzyskać nawet banalnej informacji – z powodu RODO. Zanotowano przypadki niepodpisywania kroplówek dla chorych, niewyczytywania nazwisk pacjentów w przychodniach, a także zakaz telefonicznego informowania o poszkodowanych w wypadkach drogowych. W szkołach odczytuje się listę obecności po numerach w dzienniku, a taksówkę można zamówić jedynie na hasło. W ostatnim okresie do „ofiar RODO" dołączyli podatnicy.

Inne absurdy RODO to niepodpisywanie rysunków przedszkolaków i stawianie niszczarek w urzędach, które są ponoć zgodne z nowymi wymogami. Ta psychoza zatacza coraz szersze kręgi, a urzędnicy powołują się na przepisy o ochronie danych osobowych prawdopodobnie ze strachu lub z ich nieznajomości. „Rozporządzenie nie wymaga, by korporacje taksówkarskie zastępowały nazwiska pasażerów jakimiś hasłami. To decyzja tych firm, które uznały, że w ten sposób ograniczają liczbę przetwarzanych danych i minimalizują ryzyko kłopotów w razie ich wycieku" – wyjaśnia radca prawny Tomasz Palak z kancelarii Profit Plus Prawo w Gdyni. „Gdyby taki wyciek miał miejsce, to w ręce osób niepowołanych wpadną numery telefonów i jakieś przypadkowe hasła, a nie nazwiska klientów. W tym sensie pomysł z niezbieraniem

---

[20] https://www.orange.pl/mojedane (data dostępu 1.08.2018 r.).

[21] Nowy stan prawny, uwzględniający zasady ochrony danych osobowych w RODO, został zawarty w nowej Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

[22] Por. np. rozdział IV, który zawiera szeroką wiedzę na temat przedsiębiorstwa; L. Kępa, *Ochrona danych osobowych w praktyce*, Wyd. II, Difin, Warszawa 2017.

nazwisk może dodatkowo zabezpieczać pasażerów, ale decyzja o zastosowaniu tego środka pochodzi od przedsiębiorcy, a nie wynika wprost z rozporządzenia ustawy"[23].

Po wejściu nowych przepisów bardzo trudne stało się przeglądanie Internetu. Stwierdza się, że nie jest to wina Unii Europejskiej, a wydawców. Rozporządzenie w pewnym sensie jest „desperacką, ale też konieczną próbą dostosowania przepisów do tempa, w jakim rozwijają się technologie". Afera Cambridge Analytica z Facebookiem w roli głównej dobitnie pokazała, „jakim łakomym kąskiem" są dane użytkowników. Widoczną konsekwencją dla użytkowników Internetu są wyskakujące okna informujące, kto jest administratorem ich danych, a także jakie typy danych są zbierane, poznamy nasze prawa i często znajdziemy link do polityki prywatności.

Jako przykład podano Wirtualną Polskę. „Po otwarciu strony portalu zobaczymy pop-up z wyżej wymienionymi informacjami. Gdy klikniemy *Przejdź dalej,* na dole zobaczymy mały banerek na temat plików cookies. To nie koniec. W lewym rogu zobaczymy kolejne okienko na temat polityki prywatności. Podobnie rzecz wygląda w innych portalach. Na gazeta.pl po pierwszym wejściu również wita nas analogiczny twór. Gdy otworzymy pierwszego z brzegu newsa na stronie głównej, zobaczymy kolejne okno z informacją o plikach cookies z jednej strony, a po powrocie do strony głównej ponownie, tym razem mniejsze, okienko nt. polityki prywatności". Do tego trzeba dodać „niezliczone kreacje reklamowe, w tym te bardzo inwazyjne, zasłaniające całą stronę i szybko okaże się, że z wielu polskich serwisów internetowych nie da się dziś korzystać". Z przedstawionych przykładów może jedynie wynikać, że wydawcy zastosowali się literalnie do nowych przepisów, zupełnie zapominając o użytkownikach portali internetowych[24]. Należy jednak mieć nadzieję, że są to jedynie przejściowe problemy towarzyszące tworzeniu nowej rzeczywistości prawnej.

Podsumowanie

Bieżący rok dla ochrony danych osobowych był szczególny. Na ten fakt złożyło się kilka czynników, które spowodowały niepewność, zamieszanie i wiele niejasności interpretacyjnych. Początek roku to obowiązywanie ustawy z 1997 r., maj to czas wprowadzania RODO, a następnie nowej ustawy o ochronie danych osobowych, która uwzględnia stan prawny zawarty w Rozporządzeniu 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). Dla wszystkich, którzy zajmują się prawem, jest to wyjątkowy okres dający możliwość dokonywania pierwszych ocen, interpretacji przepisów,

[23] https://www.money.pl/gospodarka/wiadomosci/artykul/rodo-histeria-firmy-wprowadzaja-absurdalne,56,0,2406968.html (dostęp 22.08.2018 r.).

[24] https://www.spidersweb.pl/2018/05/rodo-internet-portale.html (dostęp 22.08.2018 r.).

a także poszukiwania różnych nieścisłości, ponieważ żadna ustawa nie jest w stanie przewidzieć, jakie będą konsekwencje jej stosowania. Pierwsze oceny już mieliśmy po głośnym wypadku drogowym autokaru przewożącego dzieci w maju 2018 r., kiedy to ojciec nie mógł uzyskać informacji ze szpitala na temat swojego poszkodowanego dziecka. Oczywiście przeszkodą do uzyskania tego typu informacji drogą telefoniczną była ochrona danych osobowych i Rozporządzenie RODO. Tego typu interpretacji przepisów nie notowano już w następnych miesiącach.

Na stronach GIODO ukazało się wiele informacji wyjaśniających, w jaki sposób interpretować nowe przepisy. Ich głównym celem było doprowadzenie do pełnej harmonizacji prawa w ramach Unii Europejskiej i swobodnego przepływu danych osobowych. Ponadto miały pozwolić wszystkim mieszkańcom Unii Europejskiej na lepszą kontrolę ich danych osobowych, a firmom ograniczyć biurokrację i zwiększyć zaufanie swoich klientów. Przy okazji tworzenia tego prawa założono, że Rozporządzenie będzie częścią pakietu Unii Europejskiej w zakresie całościowej reformy ochrony danych. Pozostałe regulacje miały dotyczyć ochrony danych w policji i w wymiarze sprawiedliwości. Regulacje te miały być wydane w formie dyrektywy Unii Europejskiej.

W swojej treści rozporządzenie dopuszcza wprowadzenie pewnych zmian do ustawodawstwa państw członkowskich Unii Europejskiej. W Polsce nad nowymi przepisami pracowało Ministerstwo Cyfryzacji, które zaproponowało zlikwidowanie urzędu Generalnego Inspektora Ochrony Danych Osobowych i zastąpienie go Prezesem Urzędu Ochrony Danych Osobowych. W dniu 10 maja 2018 r. Sejm uchwalił nową Ustawę o ochronie danych osobowych zapewniającą stosowanie przepisów RODO na terytorium Polski. Ustawa weszła w życie z dniem 25 maja 2018 r. oraz ustanawia nowy organ w postaci Prezesa Urzędu Ochrony Danych Osobowych. Wprowadzone prawo zapewnia łatwiejszy dostęp do danych, ułatwia ich przenoszenie i przesyłanie, wprowadza nowe pojęcie – „prawo do bycia zapomnianym", nakłada na administratorów obowiązek poinformowania o ataku na posiadane przez nich dane, a także umożliwia stosowanie technologii takich jak pseudonimizacja oraz szyfrowanie. Wprowadzenie nowego aktu prawnego kończy pewien okres, który dla ochrony danych osobowych też był ważny, ale zdaniem autorów rozwiązano w ten sposób wiele wątpliwości, jakie narosły przy redagowaniu tych przepisów.

W prawie to jednak praktyka stosowania przepisów, czyli ustawy i aktów wykonawczych, które wejdą w życie po jej wprowadzeniu, da odpowiedź na pytanie, czy te zmiany faktycznie poprawiły stan ochrony danych osobowych, a przedsiębiorstwa, które są ich administratorami, cieszą się większym zaufaniem niż do tej pory. Na odpowiedź przyjdzie nam pewnie poczekać, aż ustawa zacznie spełniać swoją rolę i stanie się aktem prawnym przynoszącym same korzyści nie tylko przedsiębiorstwom.

BIBLIOGRAFIA

Akty prawa międzynarodowego:

[1] Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25).

[2] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23 listopada 1995 r.).

[3] Dyrektywa 97/66WE Parlamentu Europejskiego i Rady z dnia 15.12.1997 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w dziedzinie telekomunikacji (Dz.Urz. WE L24 z 30 stycznia 1998 r.).

[4] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (Dz.Urz. WEL 178 z 17 lipca 2000 r.).

[5] 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).

Akty Prawa Krajowego:

[1] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r., Nr 133, poz. 883 z późniejszymi zmianami).

[3] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024).

[4] Rozporządzenie MSWiA z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2004 r., Nr 94, poz. 923) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.

[5] Rozporządzenie MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., Nr 229, poz. 1536) – wydane na podstawie art. 46a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia.

[6] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r., Nr 112, poz. 1198 z późniejszymi zmianami).

[7] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 z późniejszymi zmianami).

[8] Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. z 2010 r., Nr 229, poz. 1497), ustawa weszła w życie w dniu 7 marca 2011 r.

[9] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r., Nr 159, poz. 948).

[10] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r., Nr 225, poz. 1350).

[11] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

LITERATURA

Pozycje zwarte:

[1] Barta J., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Wyd. Zakamycze 2001.

[2] Kępa L., *Ochrona danych osobowych w praktyce*, Wyd. II, Difin, Warszawa 2017.

[3] Kowalik A., *Ochrona danych osobowych*, Wyd. Sejmowe, Warszawa 2007.

[4] Kotarba W., *Ochrona wiedzy w Polsce*, Wyd. Instytut Organizacji i Zarządzania „Orgmasz", Warszawa 2005.

[5] Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999.

[6] Rybiński J., *System zarządzania innowacjami w resorcie obrony narodowej*, Wyd. WAT, Warszawa 2007.

Netografia:

[1] https://odo24.pl/blog-post.rodo-najwazniejsze-zmiany-i-nowosci-infografika

[2] http://www.orange.pl/orange_polska.phtml;osid=3D152E349831D18A37CDFB11C5C299FA.ocpwww806?_requestid=125211

[3] http://www.outsourcingportal.eu/pl/3-najwazniejsze-korzysci-z-nowej-ustawy-o-rodo

[4]]https://www.orange.pl/mojedane

[5] http://prawo.gazetaprawna.pl/artykuly/1084200,10-najwazniejszych-rzeczy-o-rodo-ktore-musisz-znac.html

[6] https://www.money.pl/gospodarka/wiadomosci/artykul/rodo-histeria-firmy-wprowadzaja-absurdalne,56,0,2406968.html

[7] https://www.spidersweb.pl/2018/05/rodo-internet-portale.html

PERSONAL DATA PROTECTION IN THE ENTERPRISE

Abstract. The legal system in force in Poland protects personal data of all Polish citizens. This system was developed along with political changes in the 90s of the last century. For several decades of its application, it was amended to create tools for a more effective and efficient system that protects the well-being of all inhabitants. Creating a system of law is the task of the Lower House and the Senate, but as a member of the European Union, Poland is also obliged to apply EU law. In this respect, legislative activity is relatively dynamic, since for many years the aim has been to introduce uniform security standards throughout the whole European Union. These standards come into force as early as of May 2018 and actually change many regulations in the existing protection rules. The aim of the paper is to present the current principles of protection and discuss the most important regulations introduced by the EU law and the effects of their application on Polish entrepreneurs.

Keywords: personal data, protection of personal data.