PRZEGLĄD ZACHODNI
2020, nr 1

KATARZYNA CHROSTOWSKA-MALAK
Warszawa
ORCID: 0000-0001-5246-5457

OCHRONA PRAWA DO PRYWATNOŚCI W POLSCE W ŚWIETLE RODO

Podobnie jak w innych państwach członkowskich Unii Europejskiej, od 25 maja 2018 r. w Polsce funkcjonuje nowy system ochrony danych osobowych (w szerokim pojęciu – część systemu ochrony prawa do prywatności), budowany na podstawie przepisów rozporządzenia 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) – dalej: RODO. Ochrona danych osobowych (a tym bardziej ochrona prawa do prywatności) nie jest nowym zagadnieniem, gdyż jej początki wiążą się z wydarzeniami tzw. rewolucji informatycznej z przełomu lat 70. i 80. XX w. W literaturze podnosi się, że „bezpośrednią przyczyną objęcia prawną ochroną danych osobowych była obawa przed pojawianiem się nowych rozwiązań technologicznych umożliwiających ich gromadzenie oraz coraz bardziej zaawansowane przetwarzanie informacji, w tym o charakterze osobowym" (Kawecki 2017: 83; Krasuski, Skolimowska 2007: 19). Na obecnym etapie, wzrost roli przetwarzania danych osobowych wynika z rosnącego potencjału nowych technologii o znaczeniu kluczowym dla rozwoju wielu krajów, stanowiący cenny materiał źródłowy dla tworzenia nowej wiedzy. Ochrona danych osobowych powiązana jest z bezpieczeństwem informacji, które należy rozumieć jako stan ochrony życiowo ważnych interesów społeczeństwa i państwa w środowisku informacyjnym od zagrożeń wewnętrznych i zewnętrznych. Bezpieczeństwo informacji to proces zabezpieczenia poufności, integralności i dostępności informacji[1]. Dodatkowo należy uwzględnić inne właściwości, tj. autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Społeczeństwo doświadcza z roku na rok wzrostu wykorzystania technologii cyfrowych m.in. w administracji publicznej. Wprowadzane są „nowe usługi dla obywateli, państwo wdraża politykę otwartych danych, udostępniając coraz większe zasoby, coraz częściej podmioty administracji sięgają po rozwiązania w chmurze". (…) Jednakże „duży stopień wykorzystania IT w administracji prowadzi do zwiększenia

[1] Są to tzw. atrybuty bezpieczeństwa informacji zgodnie z normą ISO/IEC 27001.

ryzyka w cyberprzestrzeni" (Stech 2019: 6). Działania na rzecz bezpieczeństwa w cyberprzestrzeni należą do jednych z najważniejszych obszarów zainteresowania państwa i obejmują również ochronę informacji dotyczących ludności (w tym danych osobowych)[2].

W literaturze przedmiotu podnosi się, że w Polsce po okresie transformacji ustrojowej ochrona informacji była tematyką „obcą i dość abstrakcyjną"(Gałaj-Emiliańczyk 2015:9). Dopiero 29 sierpnia 1997 r. polski parlament uchwalił ustawę o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883), która obowiązywała od 30 kwietnia 1998 r. do 24 maja 2018 r. i była uznawana za odpowiadającą międzynarodowym (europejskim) standardom. W 1999 r. Polska podpisała Konwencję nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[3], która została ratyfikowana w 2002 r. (Dz.U. 2003, nr 3, poz. 25). Akt ten stanowił przejaw demokratyzacji życia publicznego i troski państwa o prawo do prywatności każdego obywatela. System prawa Unii Europejskiej zaczął obowiązywać, a więc w przedmiocie ochrony danych osobowych była to 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.Urz. WE L 281/31). W związku ze zwiększeniem znaczenia ochrony danych w porządku prawnym UE oraz dążeniem do ujednolicenia systemów ochrony w państwach UE[4] przystąpiono do prac nad rozporządzeniem, co stanowiło kontynuację postanowień art. 16 TFUE[5], art.7 i 8 Karty Praw Podstawowych UE. RODO[6] z założenia „ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-go-

---

[2] Podstawowym aktem uchwalonym przez polski parlament, na którym opiera się system cyberbezpieczeństwa jest ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 r., poz. 1560 z późn.zm.). Celem ustawy było wdrożenie do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Państwa członkowskie zostały zobowiązane do zagwarantowania minimalnego poziomu zdolności w dziedzinie cyberbezpieczeństwa poprzez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, powołania zespołów reagowania na incydenty komputerowe (CESRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa. Ponadto z dyrektywy wynikają obowiązki służące zapewnieniu cybrebezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej.

[3] Podpisana w Strasburgu dn. 28 stycznia 1981 r. weszła w życie 1 października 1985.

[4] Na podstawie m.in. Opinii 01/2012 o projektach reformy ochrony danych przyjętej w 23 marca 2012 r. www.ec.europa.eu/justice/data-protection/index_en.htm 00530/12/PL WP 191 (dostęp:15 marca 2019 r.). Grupa Robocza została ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone zostały w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE. Na podstawie art. 68 RODO Grupę Roboczą art. 29 zastępuje Europejska Rada Ochrony Danych.

[5] Traktat o Funkcjonowaniu Unii Europejskiej (dawniej art. 286 TWE).

[6] Zgodnie z art.2 ust. 1 RODO „ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych w pod-

spodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także dla pomyślności ludzi". Zgodnie z motywem 4 RODO „przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności".

Dotychczasowy okres wdrażania nowych przepisów charakteryzował się niepewnością, chaosem informacyjnym pomieszanym niekiedy ze strachem przed wysokimi karami administracyjnymi Prezesa Urzędu Ochrony Danych Osobowych (dalej: PUODO). Po 25 maja 2018 r. byliśmy świadkami, jak nowe przepisy i zasady sprawdzają się w praktyce. Media donosiły o kolejnych tzw. absurdach RODO, przyciągających uwagę zwłaszcza, gdy dotyczyły sytuacji, w których priorytetem powinna być ochrona życia i zdrowia (szczególnie dzieci). Jeden z pierwszych takich przykładów polegał na odmowie udzielenia rodzicom informacji o stanie zdrowia dzieci, które uległy wypadkowi komunikacyjnemu na „Zakopiance"[7]. Innym absurdem RODO, o którym można się było dowiedzieć lub osobiście doświadczyć, było wywoływanie pacjentów czy również uczniów po numerach czy pseudonimach – co z kolei można byłoby kwalifikować jako działania wymierzone w ludzką godność. Kolejne, to np. likwidowanie informacji o zmarłych na nagrobkach czy zamykanie cmentarzy. Sytuacje te uzmysłowiły nam jak niebezpieczne może być niewłaściwe interpretowanie przepisów prawa, gdy odbywa się to w oderwaniu od istoty – wartości, którym mają służyć. Myślą przewodnią niniejszego opracowania jest więc stwierdzenie, że ochrona danych osobowych, choć podlega niezależnemu reżimowi prawnemu, jest nie tylko wartością samą w sobie, lecz nierzadko jest powiązana z koniecznością ochrony innych wartości.

W realizacji założonego celu konieczne będzie przedstawienie podstaw systemu ochrony prawa do prywatności w świetle RODO, a także – uwzględniając niedługą praktykę funkcjonowania przepisów RODO – próba sformułowania wniosków, które na obecnym etapie, dla dalszego rozwoju systemu ochrony danych osobowych, wydają się najistotniejsze.

---

miotach prywatnych i publicznych". Według art. 2 ust. 2 RODO „nie ma zastosowania do przetwarzania danych osobowych:

„ a) w ramach działalności nieobjętej zakresem prawa Unii;

b)przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

c) przez osobę fizyczną w ramach działalności o czysto osobistym lub domowym charakterze", czyli bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności;

„d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom".

[7] Zdarzenie z 8 czerwca 2018 r. w Tenczynie.

OCHRONA PRAWA DO PRYWATNOŚCI A OCHRONA DANYCH OSOBOWYCH

Prawo do prywatności należy do katalogu praw podmiotowych. Od dawna jest ono chronione w systemie prawa krajowego (art. 41, art. 47 Konstytucji RP, w związku z art. 31 ust. 3; szczegółowo w wielu dziedzinach prawa, w tym przede wszystkim prawa cywilnego) i międzynarodowego (ONZ, Rady Europy) oraz w prawie Unii Europejskiej. Jeden z elementów prawa do życia prywatnego stanowi prawo do dysponowania swoimi danymi osobowymi (na podstawie wyroku Sądu Apelacyjnego w Warszawie z 19 maja 2016 r. I ACa 1056/15). Na gruncie polskiego prawa w orzecznictwie sądów powszechnych podnosi się, że „reżim ochrony prawa do prywatności mieszczący się w ramach powszechnych dóbr osobistych (oparty na przepisach Konstytucji i przepisach prawa cywilnego) i reżim ochrony danych osobowych (oparty na przepisach Konstytucji oraz ustawy o ochronie danych osobowych) są wobec siebie niezależne" (Wyrok Sądu Apelacyjnego w Warszawie z 25 listopada 2016 r., sygn. akt I Ca 1565/15). Ponadto należy dodać, iż „do prywatnej sfery życia zalicza się przede wszystkim zdarzenia, okoliczności tworzące sferę życia osobistego i rodzinnego. Nie każda informacja dotycząca określonej osoby jest informacją z dziedziny jej życia osobistego"(Tamże).

Ochrona życia prywatnego gwarantowana jest w art. 41 Konstytucji i „obejmuje sformułowaną przez Trybunał Konstytucyjny (TK) autonomię informacyjną (art. 51 Konstytucji RP), która oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, jak również prawo sprawowania kontroli nad takimi informacjami jeśli znajdują się one w posiadaniu innych podmiotów" (Wyrok TK z 19 lutego 2002 r., sygn. U 3/01; Wyrok TK z 26 czerwca 2008 r., sygn. K 8/04). W świetle obowiązującego prawa, na co wskazuje również orzecznictwo sądów powszechnych „jednostka, jako podmiot obdarzony autonomią woli, ma prawo samodzielnie wyznaczać obszar swojej prywatności, w szczególności wytyczać granice dostępności swojego życia osobistego dla innych" (Wyrok Sądu Apelacyjnego w Warszawie z 12 listopada 2013 r., sygn. Akt I ACa 906/13). W innym wyroku z 21 września 2005 r., tym razem Wojewódzki Sąd Administracyjny orzekł, że stosując przepisy ustawy o ochronie danych osobowych, należy „za każdym razem wyważyć dobra, które legły u jej podstaw. Prawo do ochrony danych osobowych, jako jeden z elementów prawa do własnej prywatności, ma swoje źródło w przepisach art. 47, art. 49, art. 50 i art. 51 Konstytucji RP. Istotnym elementem prawa do prywatności są konstytucyjnie ustanowione ograniczenia dotyczące ujawnienia, pozyskiwania i dostępności informacji o osobach prywatnych (art. 51). W praktyce prawo do ochrony danych osobowych ulega ograniczeniu z uwagi na interes publiczny lub usprawiedliwiony interes innych osób, czyli nie jest to prawo o charakterze absolutnym, jak większość praw chronionych konstytucyjnie" (Sygn. akt II SA/Wa 1443/05). Podobnie w wyroku z 22 marca 2011 r. Naczelny Sąd Administracyjny wyraził pogląd, że wolności gwarantowane bezpośrednio przez Konstytucję nie mają charakteru absolutnego, co wynika z „przyjętej w Konstytucji RP zasady proporcjonalności (art. 31 ust. 3) oraz z treści samego art. 51 Konstytucji RP. Zgodnie z tym ostatnim przepisem każdy jest właścicielem i dysponentem własnych danych osobowych. Pewne ograniczenia

tej zasady są jednak dopuszczalne, z tym że zostały one zastrzeżone do regulacji ustawowej" (Sygn. akt I OSK 623/10).

Prawo do prywatności (w tym ochrona danych osobowych) nabiera szczególnego znaczenia w przypadku gdy dotyczy np. pacjenta[8], czyli osoby zwracającej się o udzielenie świadczeń zdrowotnych lub korzystającej ze świadczeń podmiotu lub osoby ich udzielającej, w trakcie których dochodzi do przetwarzania szczególnej kategorii danych osobowych (tzw. wrażliwych). ETPCz wyjaśnia, że „pojęcie 'życia prywatnego' w rozumieniu art. 8 Konwencji jest pojęciem szerokim, które obejmuje między innymi prawo do ustanowienia i rozwijania relacji z innymi ludźmi. Obejmuje takie elementy jak życie seksualne oraz, bezsprzecznie, informacje osobiste dotyczące pacjenta" (Wyrok ETPCz z 25 listopada 2008 r. 23373/03). Ochronie tej od dawna służy tajemnica lekarska (zawodowa). Orzecznictwo ETPCz potwierdza „informacje osobiste dotyczące pacjenta wchodzą w zakres jego życia prywatnego. Ochrona danych osobowych, także danych medycznych, ma podstawowe znaczenie dla korzystania przez osobę z jej prawa do poszanowania życia prywatnego i rodzinnego gwarantowanego przez art. 8 Konwencji" (Wyrok ETPCz z dnia 25 listopada 2008 r. 23373/03). W jednym z najnowszych orzeczeń, Trybunał stwierdził

> „poszanowanie poufności danych dotyczących stanu zdrowia jest ważną zasadą w systemach prawnych wszystkich Układających się Stron Konwencji. Zasadnicze znaczenie ma nie tylko poszanowanie poczucia prywatności pacjenta, ale także ochrona zaufania pokładanego przez niego w zawodzie lekarza oraz ogólnie w służbie zdrowia. Bez takiej ochrony osoby potrzebujące opieki medycznej mogą obawiać się ujawnienia informacji o charakterze osobistym i intymnym, koniecznych dla uzyskania odpowiedniego leczenia, a nawet obawiać się korzystania z pomocy medycznej, ryzykując tym samym własnym zdrowiem, a w przypadku chorób zakaźnych – zdrowiem społeczności. Prawo krajowe musi zatem przyznawać odpowiednie gwarancje w celu uniemożliwienia takiego przekazywania lub ujawniania danych osobowych dotyczących stanu zdrowia, które mogą być niezgodne z gwarancjami art. 8 Konwencji" (wyrok ETPCz z 27 lutego 2018 r. 66490/09).

W podobny sposób Europejski Trybunał Praw Człowieka wypowiedział się w wyroku z 27 sierpnia 1997 r. (20837/92).

Problematyce bezpieczeństwa ochrony danych o stanie zdrowia poświęcono wiele uwagi w licznych rekomendacjach Komitetu Ministrów oraz Zgromadzenia Parlamentarnego Rady Europy (Sobczak 2013:207-272).

OCHRONA DANYCH OSOBOWYCH

W polskim systemie prawa ochrona danych osobowych wynika z przepisów:

- Konstytucji Rzeczypospolitej Polskiej (art. 47 i 51 Konstytucji);
- Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności – art. 8 stanowi, że „każdy ma prawo do poszanowania swojego życia prywatnego i ro-

[8] Patrz: ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta – t.j. Dz.U. z 2017 r., poz.1318, 1524 z późn. zm.

dzinnego, swojego mieszkania (ang. *home*) i swojej korespondencji". Postanowienie to było inspirowane art. 12 Powszechnej Deklaracji Praw Człowieka (Czubik 2013: 294);
- Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (data uchylenia: 1 kwietnia 2019 r.) zastąpioną Konwencją nr 108 +;
- Traktatu o funkcjonowaniu Unii Europejskiej (art. 16 ust. 1) i Karty Praw Podstawowych Unii Europejskiej (art. 7 i 8 ust. 1);
- Rozporządzenia 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*)* – jest aktem prawnym obowiązującym bezpośrednio, niewymagającym implementacji;
- Ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000) jako podstawowego aktu prawa krajowego *doprecyzowującego przepisy RODO* (Dmochowska, Piotrowska, 2018: XVII).

Co do zasady, ustawy o ochronie danych osobowych oraz RODO na podstawie art. 6 tej ustawy nie stosuje się „w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego" i innych, wskazanych w tym artykule sprawach (dotyczących działalności służb specjalnych). Przepisy stosowane na zasadzie *lex specialis* zawarte są w ustawach:
- z 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2018 r. poz. 412, 650, 1000, 1083, 1669, z 2019 r. poz. 125)[9];
- z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125 z późn. zm.), która określa

> „zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności".

oraz są rozproszone w innych aktach normatywnych (np. w art. 6 ustawy z 24 maja 2000 r. o Krajowym Rejestrze Karnym).

W sytuacji, gdy wprost z przepisów nie wynikają wyłączenia, należy stosować ogólne zasady znane prawu konstytucyjnemu oraz międzynarodowemu (przede wszystkim te, o których mowa w art. 31 ust. 3 Konstytucji RP).

O ile przepisy RODO nie podlegają implementacji, to w związku z koniecznością harmonizacji na poziomie prawa krajowego zaistniała potrzeba usunięcia z polskie-

[9] Zgodnie z jej postanowieniami (art.1 ust.4), ustawy o ochronie danych osobowych nie stosuje się do danych osobowych stanowiących informacje niejawne. Na podstawie art. 1 ust. 5 ustawy, do danych osobowych stanowiących informacje niejawne stosuje się przepisy o ochronie informacji niejawnych.

go systemu prawa przepisów sprzecznych lub powielających rozwiązania RODO[10]. Celem nowego prawa było również uszczegółowienie rozwiązań z RODO w różnych dziedzinach. W związku z powyższym Ministerstwo Cyfryzacji przygotowało projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (liczący 216 stron, zaś samo uzasadnienie – 287 stron). Projektowane zmiany dotyczyły w sumie 168 ustaw. Prezydent Rzeczypospolitej Polskiej podpisał 3 kwietnia 2019 r. ustawę z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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). Ustawa zmieniająca przewiduje nowelizację 162 ustaw.

Prawa i wolności jednostki, jeżeli mają być realizowane, powinny być chronione przed zagrożeniami i naruszeniami. Zagrożenia praw i wolności jednostki to czynniki ograniczające całkowicie możliwości ich realizacji lub utrudniające tę realizację (Banaszak 2017:393). Ochronę praw i wolności jednostki stanowi ogół środków oraz działalność mająca na celu ich zapewnienie i realizację poprzez zabezpieczenie przed ich naruszeniem oraz przeciwdziałanie ich zagrożeniom (Tamże: 394). Oceniając, czy nastąpiło wkroczenie w dziedzinę chronionego prawem życia prywatnego, nie należy pojęcia tego absolutyzować, bowiem ze względu na stopień ogólności, wymaga ono wykładni przy uwzględnieniu konkretnych okoliczności charakteryzujących daną sytuację. RODO daje podstawy do rozbudowy systemu ochrony danych osobowych zachowując najbardziej sprawdzone dotąd podstawowe zasady przetwarzania danych. Nowe przepisy wymusiły na podmiotach im podlegających: przyjęcie nowych polityk bezpieczeństwa danych osobowych (polityk prywatności), kodeksów, przeprowadzenie analizy ryzyka przetwarzania danych osobowych, spełnienia obowiązku informacyjnego z art. 13 i 14 RODO, zawarcia umów powierzenia przetwarzania danych osobowych, prowadzenia rejestrów czynności przetwarzania danych, rejestrów kategorii czynności i innych. Przystosowanie różnorodnych podmiotów do RODO wymagało także wzmocnienia środków bezpieczeństwa przetwarzanych danych z art. 32 RODO czy też podjęcia innych działań organizacyjnych (np. w podmiotach leczniczych wydzielenia specjalnych miejsc rejestrowania pacjentów czy też udzielania informacji dotyczących stanu zdrowia i decyzji dotyczących dalszego leczenia), co zazwyczaj oznaczało konieczność poniesienia dodatkowych nakładów finansowych.

Jedynym organem w Polsce w sprawach ochrony danych osobowych, posiadającym jednocześnie status organu nadzorczego, o którym mowa w RODO jest Prezes Urzędu Ochrony Danych Osobowych (PUODO). Postępowanie administracyjne przed tym organem jest jednoinstancyjne.

---

[10] Uzasadnienie do ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (druk sejmowy 3050).

Dla potrzeb niniejszego artykułu poniżej zostaną wyjaśnione (zdefiniowane) najczęściej występujące w opracowaniu pojęcia, kluczowe w systemie ochrony danych osobowych RODO.

Dane osobowe – są to wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W świetle jurydycznej definicji danymi osobowymi będą zatem zarówno takie informacje, które pozwalają na określenie tożsamości konkretnej osoby, jak i te, które nie pozwalają na jej natychmiastową identyfikację, ale są – przy pewnym nakładzie kosztów, czasu i działań – wystarczające do jej ustalenia (np. imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, jeden lub kilka czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej). Rozróżniamy dwie podstawowe grupy danych osobowych: dane osobowe zwykłe i dane osobowe szczególnych kategorii (zwane również wrażliwymi).

– Dane osobowe zwykłe obejmują: imię i nazwisko, adres, lokalizacja, identyfikator internetowy, nr telefonu, adres e-mail, i inne, nienależące do kategorii danych szczególnych, a umożliwiające identyfikację osoby fizycznej. Katalog danych osobowych zwykłych, w przeciwieństwie do katalogu danych osobowych wrażliwych, jest katalogiem otwartym. Przykładowo zgodnie z wyrokiemTrybunału Sprawiedliwości UE z 20 grudnia 2017 r. w sprawie C-434/16 Peter Nowak vs. Data Protection Commissioner pojęcie danych osobowych obejmuje również „pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi" *(InfoCuria – Orzecznictwo Trybunału Sprawiedliwości: www.curia.europa.eu/juris/recherche.jsf?language=pl*, dostęp 31.03.2019).
– Dane osobowe szczególnych kategorii (wrażliwe) to informacje dotyczące: stanu zdrowia (w tym także informacja o korzystaniu z usług placówki medycznej o określonej specjalizacji, np. psychiatrycznej), pochodzenia rasowego lub etnicznego, poglądów politycznych, przynależności do związków zawodowych, danych genetycznych, danych biometrycznych dających możliwość jednoznacznego zidentyfikowania osoby fizycznej, orientacji seksualnej.

Na gruncie RODO katalog danych wrażliwych uległ zmianie. W szczególności został on poszerzony o dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej.

Podkreślić także należy, że RODO odrębnie reguluje dane dotyczące wyroków skazujących oraz czynów zabronionych. O ich szczególnym statusie prawnym rozstrzyga w odrębnej regulacji, tj. w art. 10 rozporządzenia, który dopuszcza przetwarzanie takich danych osobowych na podstawie przesłanek wynikających z art. 6 ust. 1, jedynie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Przetwarzanie – to wszelkie działania wykonywane na danych osobowych (prowadzone w sposób zautomatyzowany lub niezautomatyzowany), takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub mo-

dyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie.

Podmiotem, który ustala cele i sposoby przetwarzania danych osobowych jest **administrator**. Może nim być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot. W literaturze podkreśla się, że „pojęcie administratora ma kluczowe znaczenie dla stosowania przepisów rozporządzenia 2016/679, ponieważ to administrator jest adresatem szeregu obowiązków wynikających z tego aktu prawnego" (Witkowska-Nowakowska 2018: 211). Zgodnie z art. 4 pkt 7 RODO „administrator może być podmiotem funkcjonującym w dowolnej formie prawnej dającej mu zdolność do nabywania praw i zaciągania zobowiązań i związaną z tym możliwość ustalania celów i sposobów przetwarzania" (Krzysztofek 2016: 204).

Tak więc administrator może być podmiotem należącym do sektora prywatnego lub publicznego, osobą fizyczną lub prawną (tj. spółki kapitałowe, spółdzielnie, stowarzyszenia, fundacje), organem publicznym (tj. państwowe, samorządu terytorialnego oraz inne państwowe i komunalne jednostki organizacyjne), jednostką organizacyjną nieposiadającą osobowości prawnej lub innym podmiotem" (Tamże). W sektorze publicznym, często o tym, kto jest administratorem, decydują przepisy sektorowe np. dotyczące działu administracji rządowej, powierzające organom konkretne zadania i kompetencje.

Należy jednak pamiętać, że zapewnianie zgodności z prawem przetwarzania danych osobowych, jak również ponoszenie odpowiedzialności za działania wszystkich osób upoważnionych do przetwarzania danych osobowych w konkretnym podmiocie (organizacji) ciąży na osobie ją reprezentującej. Właściwe zarządzanie danymi osobowymi stanowi element odpowiedzialnego oraz dobrego zarządzania organizacją. Wdrażając natomiast jakikolwiek system ochrony informacji, należy brać pod uwagę specyfikę działalności konkretnego podmiotu oraz czynnik ludzki. Dlatego istotne jest budowanie właściwej świadomości wśród członków organizacji, np. poprzez szkolenie personelu.

Podmiot przetwarzający (inaczej procesor) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (na podstawie upoważnienia, umowy lub innego instrumentu prawnego).

W oparciu o wykładnię Grupy Roboczej art. 29 „istnienie podmiotu przetwarzającego uzależnione jest od spełnienia dwóch warunków. Po pierwsze, podmiot ten ma być odrębnym bytem prawnym od administratora. Po drugie, musi wykonywać operacje przetwarzania danych w imieniu administratora" (Witkowska-Nowakowska 2018: 225). Status procesora uzyskuje podmiot w efekcie powierzenia (zlecenia) mu przetwarzania danych np. przy okazji realizacji umowy. Powierzenie (zlecenie) przetwarzania danych następuje w drodze umowy[11] między podmiotem przetwarza-

[11] Umowa powierzenia, o której mowa powyżej, powinna zawierać określone elementy, tj. dane administratora i procesora; zezwolenie na przetwarzanie powierzonych procesorowi danych osobowych; przedmiot i czas trwania przetwarzania danych, w tym określenie rodzaju danych osobowych i kategorii osób, które one dotyczą; zakres i charakter oraz cel przetwarzania; obowiązki i prawa administratora,

jącym a administratorem. Niemniej jednak należy mieć na uwadze, że „w pewnych okolicznościach istnienie relacji powierzenia nie wynika z autonomicznej decyzji administratora, lecz z instrumentów prawnych regulujących dane przetwarzanie. Taki przypadek występować może w sferze publicznej" (Witkowska-Nowakowska 2018: 225). W przetwarzaniu danych osobowych może brać udział również podprocesor, który jest podmiotem przetwarzającym dane w imieniu administratora na podstawie umowy zawartej z procesorem. Za jego działania odpowiada procesor.

Przepisy RODO wymagają, że jeśli przetwarzanie ma być dokonywane w imieniu administratora (np. na podstawie umowy powierzenia przetwarzania danych osobowych), korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE

Podmiot przetwarzający dane osobowe (administrator, procesor, podprocesor, i inne) zobowiązany jest do przestrzegania zasad ochrony danych osobowych, w tym m.in. do:

1) spełnienia obowiązku informacyjnego z art. 13 i 14 RODO względem osób, których dane osobowe przetwarza (np. poprzez udzielanie informacji odnośnie celów, podstaw prawnych, sposobów, źródeł, zakresu przetwarzania danych osobowych, itp.);
2) upoważnienia do przetwarzania danych osobowych osób, które biorą w nim udział oraz zobowiązaniu tych osób do zachowania w tajemnicy pozyskiwanych w tym procesie informacji o osobach fizycznych;
3) dbałości o bezpieczeństwo danych osobowych poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zabezpieczenia danych osobowych, aby dane te nie były udostępniane osobom nieupoważnionym oraz były chronione przed zniszczeniem albo utratą (w szczególności poprzez szyfrowanie danych, pseudonimizację, zapewnienie integralności i poufności danych);
4) respektowania praw osób, których dane są przetwarzane (m.in. poprzez spełnianie żądań sprostowania, uaktualnienia albo uzupełnienia czy też zaprzestania ich przetwarzania).

Administrator może wyznaczyć inspektora ochrony danych (IOD), co zostało przewidziane w art. 37 RODO. Dane inspektora ochrony danych (w tym dane kontaktowe) powinny być opublikowane na stronach internetowych podmiotu. Informacje o jego powołaniu powinny być zgłoszone organowi nadzorczemu, czyli PUODO.

---

w tym prawo do kontroli procesora; obowiązki i prawa podmiotu przetwarzającego; informację o możliwości i warunkach dalszego powierzenia danych innemu podmiotowi przetwarzającemu (podprocesorowi); postanowienia dotyczące odpowiedzialności podmiotu przetwarzającego; czas obowiązywania umowy; zasady zachowania poufności.

INSPEKTOR OCHRONY DANYCH

Wyznaczenie Inspektora Ochrony Danych (IOD) jest co do zasady uprawnieniem administratora. W sytuacjach jednak przewidzianych w art. 37 ust. 1 lit. a RODO wyznaczenie IOD staje się obowiązkiem administratora – administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

Inspektorem ochrony danych może być osoba zatrudniona na podstawie umowy o pracę, umowy o świadczenie usług, outsourcingu. Funkcja ta może być powierzona również osobie, która zatrudniona jest w organizacji na innym stanowisku, jednakże administrator musi zapewnić, żeby powierzone jej zadania i obowiązki nie doprowadzały do konfliktu interesów (art. 38 ust. 6 RODO).

Jeżeli administrator lub podmiot przetwarzający jest organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć jednego inspektora ochrony danych osobowych w zależności od struktury organizacyjnej i wielkości podmiotu.

RODO wymaga od inspektora posiadania fachowej wiedzy na temat prawa oraz praktyki w zakresie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO. W literaturze przedmiotu podkreśla się, że IOD pełni rolę punktu kontaktowego. „Rola punktu kontaktowego jest mocno powiązana z obowiązkami administratora oraz podmiotu przetwarzającego i ma przyczyniać się do skuteczniejszego ich wykonywania" (Młotkiewicz 2018:20). Osoby, których dane osobowe są przetwarzane zgodnie z art. 38 ust. 4 RODO, są uprawnione „do kontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO" (Tamże:21). Jego stanowisko ma mieć z założenia samodzielny i niezależny charakter. Pomocne w określeniu statusu IOD są m.in. wytyczne dotyczące inspektorów ochrony danych ('DP') przyjęte w dniu 13 grudnia 2016 r. ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r. Grupa Robocza art. 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (http://ec.europa.eu/justice/data-protection/index_en.htm, dostęp 31.03.2019).

ZASADY WIĄŻĄCE WSZYSTKIE WYMIENIONE PODMIOTY BIORĄCE UDZIAŁ W PRZETWARZANIU DANYCH OSOBOWYCH (ART. 5 RODO)

Nowe przepisy umacniają dotychczas funkcjonujące zasady w ochronie danych osobowych, formułują też inne. Katalog zasad, o których mowa jest następujący:

– Zasada zgodności z prawem, rzetelności i przejrzystości – oznacza ona, że dane osobowe muszą być przetwarzane w ramach obowiązującego prawa, rzetelnie i w sposób przejrzysty dla osoby, której one dotyczą;

- Zasada ograniczenia celu przetwarzania – zbieranie danych osobowych musi odbywać się w konkretnych, wyraźnych i prawnie uzasadnionych celach; niedozwolone jest dalsze przetwarzanie danych w sposób niezgodny z tymi celami (przy czym dalsze przetwarzanie danych do celów archiwalnych w interesie publicznym, badań naukowych lub historycznych lub statystyki nie jest uznawane za niezgodne z pierwotnymi celami);
- Zasada adekwatności (minimalizacja danych) – oznacza, że gromadzone dane muszą być adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do osiągnięcia celów, w których są przetwarzane;
- Zasada prawidłowości – wymaga, ażeby dane były prawidłowe i w razie potrzeby uaktualnione. W przypadku wystąpienia nieprawidłowych danych w świetle celów ich przetwarzania, należy niezwłocznie usunąć lub sprostować nieprawidłowości;
- Zasada ograniczenia przechowywania – dane osobowe mogą być składowane w formie umożliwiającej identyfikację osoby, której dotyczą, tylko przez okres niezbędny do celów, dla których są przetwarzane. Dłuższe przetwarzanie jest możliwe wyłącznie do celów archiwalnych w interesie publicznym, badań naukowych, historycznych lub statystycznych;
- Zasada integralności i poufności – przetwarzanie powinno odbywać się w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem lub przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- Zasada rozliczalności – w myśl tej zasady administrator danych osobowych (również podmiot działający z jego upoważnienia) jest odpowiedzialny za przestrzeganie wszystkich powyższych zasad. Musi on być w stanie wykazać, że przestrzegał tych reguł (rozliczalność). Zasada ta kładzie nacisk na zastosowanie w praktyce odpowiednich procedur i innych działań służących ochronie danych osobowych.

OBOWIĄZEK INFORMACYJNY

Artykuł 13 i 14 RODO nakłada na administratorów obowiązek informowania osób fizycznych, których dane są przetwarzane (pracowników, kandydatów do pracy, kontrahentów) o swojej tożsamości i danych kontaktowych, danych inspektora ochrony danych, celach przetwarzania i podstawie prawnej oraz przysługujących prawach, którymi są:

- Prawo do informacji o przetwarzaniu, w tym informowania o celach, terminach, i odbiorcach przetwarzania danych osobowych;
- Prawo dostępu do danych, tj. prawo do wglądu oraz prawo do żądania przekazania kopii wszystkich danych na temat wnioskodawcy znajdujących się w posiadaniu administratora;

– Prawo do sprostowania lub uzupełnienia danych, które są nieprawidłowe (zgodnie z art. 16-RODO). Ponadto, każdy ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia;
– Prawo sprzeciwu wobec przetwarzaniu danych – osoby, których dane są przetwarzane w interesie publicznym lub w związku z uzasadnionym interesem administratora, mogą się temu sprzeciwić, chyba że administrator wykaże, iż podstawa do przetwarzania danych jest nadrzędna w stosunku do interesów jednostki;
– Prawo do usunięcia danych tzw. prawo do bycia zapomnianym (art. 17 RODO) – osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego ich usunięcia, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z określonych okoliczności;
– Prawo do przenoszenia danych (art. 20 RODO) w praktyce oznacza, że osoba ma prawo: otrzymać dane, które jej dotyczą – w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego; nakazać przekazanie tych danych innemu administratorowi (prawo to ma zastosowanie, gdy dane są przetwarzane na podstawie zgody lub w celu wykonania umowy; gdy przetwarzanie danych odbywa się w sposób zautomatyzowany);
– Prawo wnoszenia skarg do organu nadzorczego – tj. do PUODO.

LEGALNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

Legalność przetwarzania danych osobowych zwykłych

Na podstawie art. 6 RODO do przetwarzania danych osobowych zwykłych uprawnia spełnienie jednej z przesłanek:

– osoba, której dane dotyczą wyraziła na to zgodę[12] w sposób dobrowolny, konkretny, świadomy i jednoznaczny (przy jednoczesnym zachowaniu wymogu minimalizacji danych osobowych). Co do zasady tę przesłankę stosuje się w sytuacji, gdy nie występują inne niżej wskazane;
– przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
– przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
– przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

[12] Więcej na temat zgody – patrz poniżej.

– przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
– przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Każda z wyżej wymienionych przesłanek ma charakter autonomiczny i może stanowić samodzielną podstawę przetwarzania danych osobowych. W podmiotach publicznych przetwarzanie danych osobowych najczęściej odbywa się na podstawie przepisów prawa i jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

OBOWIĄZEK UZYSKANIA ZGODY

Trybunału Sprawiedliwości Unii Europejskiej w wyroku z dnia 15 marca 2017 r. wskazał, że zgoda na przetwarzanie danych osobowych może być wyrażana w sposób odmienny w zależności od państwa członkowskiego (Wyrok TSUE z dnia 15 marca 2017 r., C- 536/15).

Zgoda osoby, której dane dotyczą, na przetwarzanie jej danych osobowych jest oświadczeniem (okazaniem) woli i można ją wyrażać na różne sposoby, nie zawsze w formie pisemnej. „Oświadczenie woli o zgodzie jest konstrukcją prawną zbliżoną do oświadczenia woli w rozumieniu kodeksu cywilnego" (Fajgielski 2018: 127). RODO inaczej niż art. 60 kodeksu cywilnego[13] (dalej: k.c.) mówi o oświadczeniu lub działaniu potwierdzającym.

Według wytycznych Grupy Roboczej art. 29

> „co do zasady zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji. Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda w pełni odpowiadająca RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy będą one przetwarzane"[14].

Specyficzną jest zgoda na publikowanie zdjęć np. na stronie internetowej. Zagadnienie to wiąże się nie tylko z ochroną danych osobowych, lecz także – w związku z rozpowszechnianiem wizerunku – podlega przepisom art. 81 ust.1 ustawy o prawie

[13] Ustawa z 23 kwietnia 1964 r. – kodeks cywilny (Dz.U. 2018 r. poz.1025 z poźn. zm.).

[14] Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 przyjęte 28 listopada 2017 r. Ostatnio zmienione i przyjęte 10 kwietnia 2018 r. – www.uodo.gov.pl/pl/10/428 (dostęp 29 marca 2019 r.).

autorskim i prawach pokrewnych[15] i wymaga zezwolenia osoby, której dotyczy. Ponadto, niezależnie od powyższego, wizerunek pozostaje pod ochroną prawa cywilnego – art. 23 k.c.

Na podstawie art. 7 ust. 3 RODO osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. W związku z powyższym, przepisy nakładają na administratora obowiązek poinformowania o tym prawie osoby, której dane dotyczą, zanim wyrazi zgodę. Skorzystanie z tego uprawnienia musi być równie łatwe jak wyrażenie zgody.

LEGALNOŚĆ PRZETWARZANIA SZCZEGÓLNEJ KATEGORII DANYCH OSOBOWYCH (TZW. WRAŻLIWYCH)

Przetwarzanie danych osobowych wrażliwych – co do zasady ogólnej wyrażonej w art. 9 ust. 1 RODO – jest zabronione. Wyjątkowo, na podstawie art. 9 ust. 2, zakaz tan nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba, że prawo przewiduje, iż osoba nie może uchylić zakazu;
- przetwarzanie jest niezbędne do wypełniania obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem;
- przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażania zgody;
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem, że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- gdy dotyczy danych osobowych w sposób oczywity upublicznionych przez osobę, której dotyczą;
- gdy jest ono niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa, proporcjonalnie do wyznaczonego celu, nie

[15] Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 2018 r. poz. 1191 z późn. zm.).

narusza istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
– przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa lub zgodnie z umową z pracownikiem służby zdrowia (z obowiązkiem zachowania tajemnicy);
– przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym do celów badań naukowych lub historycznych lub do celów statystycznych.

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 32 RODO stanowi, że

„uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi:

a) pseudonimizację i szyfrowanie danych osobowych;
b) zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (…)".

RODO nie zawiera szczegółowych wymogów dotyczących organizacyjnego i technicznego zabezpieczenia danych osobowych, lecz określa jedynie ogólne zasady w tym zakresie. Środki te powinny być dostosowane do zidentyfikowanych ryzyk w organizacji oraz uwzględniać aktualny stan wiedzy w tym zakresie. W związku z powyższym zastosowanie będą miały normy systemów zarządzania bezpieczeństwem informacji: PN ISO/IEC 27000, 27001, 27002, 27005. Podmioty publiczne powinny wziąć pod uwagę również wymogi określone przepisami rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017 r. poz. 2247).

ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH

Nowym obowiązkiem administratora nałożonym przepisem art. 33 RODO, a zarazem uprawnieniem współdziałania z organem nadzorczym, jest zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego, którym jest PUODO. Należy

zauważyć przy tym, że „każde naruszenie ochrony danych jest incydentem, ale nie każdy incydent stanowi naruszenie w rozumieniu przepisów o ochronie danych osobowych" (Mazur 2018: 22-23).

Naruszenie ochrony danych w myśl art. 4 pkt 12 RODO polega na naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

RODO zobowiązuje również administratora do powiadomienia o zdarzeniu „bez zbędnej zwłoki" osoby fizycznej, której dane zostały naruszone, a więc tak szybko, jak tylko pozwalają na to okoliczności. Działanie to ma na celu podjęcie niezbędnych działań zapobiegawczych dla ochrony przed negatywnymi skutkami naruszenia. Przykładem może być wyciek haseł klienta sklepu internetowego lub banku.

Za naruszanie przepisów RODO przewiduje wysokie kary administracyjne dla administratorów. Są one nakładane w postępowaniach jednoinstancyjnych prowadzonych przez PUODO[16]. Ponadto ustawodawca przewidział kary dla osób fizycznych za nieprzestrzeganie zasad i przepisów wynikających z ustawy z 10 maja 2018 r. o ochronie danych osobowych. Zgodnie z jej postanowieniami:

> „Art.107.1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
>
> 2. Jeśli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących ochrony zdrowia, seksualności i orientacji seksualnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech".

ZAKOŃCZENIE

Proces wdrażania przepisów RODO wymagał i wymaga wciąż wielu działań o charakterze legislacyjnym[17], administracyjnym i organizacyjnym na szczeblu ogól-

---

[16] Pierwsza kara pieniężna PUODO (w wysokości ponad 943 tys. zł.) dotyczyła niedopełnienia obowiązku informacyjnego – patrz na ten temat m.in.: www.uodo.gov.pl/pl/138/786 (dostęp: 28.03.2019).

[17] W trakcie transpozycji przepisów RODO do prawa krajowego zaznaczyły się rozbieżności co do ich właściwej interpretacji, również na szczeblu centralnym. Spór o właściwą wykładnię dotyczył np. prawa dostępu do dokumentacji medycznej realizowanego na podstawie polskiego prawa (ustawy o prawach pacjenta), w którym należało uwzględnić respektowanie dwóch praw podstawowych: prawa do informacji o stanie zdrowia i praw z zakresu ochrony danych osobowych. Rzecznik Praw Obywatelskich i PUODO wydali sprzeczne w tym zakresie opinie. Rzecznik Praw Obywatelskich w swoim stanowisku z dnia 25 maja 2018 r. wskazał, że „pacjenci na kanwie RODO mają m.in. prawo dostępu do swoich danych osobowych, które mogą zrealizować poprzez żądanie kopii. Placówki medyczne przetwarzają dane osobowe dotyczące stanu zdrowia pacjentów w szczególności w prowadzonej dokumentacji medycznej. Wykonując obowiązek będą zobowiązane do bezpłatnego udostępniania pierwszej kopii dokumentacji

nopaństwowym, w administracji rządowej, a w szczególności w podmiotach publicznych i prywatnych zobligowanych przepisami RODO. W proces ten zaangażowane są najwyższe organy władzy państwowej: parlament, rząd (w tym ministrowie resortowi, przede wszystkim minister cyfryzacji), organy centralne (PUODO) i wiele innych podmiotów i instytucji. Przed 25 maja 2018 r. nagłaśniano konieczność przygotowania podmiotów publicznych i prywatnych do RODO, a zbudowane dotychczas systemy ochrony danych osobowych są wciąż doskonalone.

Wkraczamy jednak w fazę większej pewności prawnej działania. Zmiany obserwowane w związku z RODO w zakresie ochrony prawa do prywatności poprzez wzmocnienie systemów ochrony danych osobowych należy postrzegać jak najbardziej pozytywnie. Mówi się, że RODO jest inteligentnym dokumentem wymagającym inteligentnej interpretacji i stosowania. Decydującym czynnikiem wpływającym na bezpieczeństwo danych w świetle RODO pozostaje więc czynnik ludzki. Niemniej jednak, ze względu na coraz częstsze przetwarzanie danych osobowych w systemach teleinformatycznych (czemu towarzyszy ryzyko wystąpienia zagrożenia dla bezpieczeństwa informacyjnego), niezmiernie ważne jest również odpowiednie zabezpieczenie tych systemów.

W pierwszym roku obowiązywania RODO zaznaczyła się rola IOD (dawniej ABI), nie tylko jako tzw. punktu kontaktowego. Niejednokrotnie okazuje się, że między innymi również poprzez przejmowanie obowiązków administratora, system ochrony danych w poszczególnych organizacjach tworzy i doskonali IOD. Nie bez znaczenia jest fakt, iż wiele inicjatyw PUODO (szkolenia, warsztaty, infolinia, poradniki) było adresowanych właśnie do Inspektorów.

Dotychczasowa praktyka pokazała, jak niebezpieczne może okazać się niewłaściwe interpretowanie przepisów prawa, gdy dokonywane jest w oderwaniu od jego istoty. W indywidualnym podejściu do każdej sprawy (bo tego wymaga RODO), gdy pojawiają się wątpliwości co do hierarchii dóbr, które należy wziąć pod ochronę,

---

medycznej". PUODO natomiast w stanowisku z 27 lipca 2018 r. stwierdził, że „udostępnienie kopii danych zawartych w dokumentacji medycznej, zgodnie z art. 15 ust. 3 RODO, nie jest równoznaczne z obowiązkiem udostępnienia danych w formie i strukturze właściwych dla udostępnienia dokumentacji medycznej". Wobec powyższego, mając na uwadze szczególny charakter omawianej materii, projektodawca zdecydował się na zrównanie uprawnień wynikających w tym zakresie z RODO oraz przepisów prawa krajowego, biorąc pod uwagę również motyw 63 RODO.

Inny przykład dotyczył rozstrzygnięcia przesłanki uprawniającej pracodawców do przechowywania dokumentacji z rekrutacji pracowniczej i rozstrzygnięć Ministerstwa Cyfryzacji zawartych w art. 33 Prawa przedsiębiorców. PUODO stwierdził, że „po zakończeniu rekrutacji dane osobowe kandydatów powinny być niezwłocznie usunięte – chyba, że ze względu na zainteresowanie przyszłymi rekrutacjami wyrażą zgodę na dłuższe ich przechowywanie" – w: Poradnik RODO „Ochrona danych osobowych w miejscu pracy": https://uodo.gov.pl/pl/file/1469. Ministerstwo Cyfryzacji w formalnym objaśnieniu zaprezentowanym na briefingu prasowym 23 stycznia 2019 r., w związku z regulacją art. 33 Prawa przedsiębiorców przedstawił odmienne stanowisko niż PUODO – mianowicie, że dokumentacja z rekrutacji pracowniczej może być przechowywana przez przedsiębiorców (na podstawie przesłanki prawnie uzasadnionego interesu administratora art. 6 ust. 1 lit. f), w razie ewentualnych roszczeń kandydatów z tytułu np. dyskryminowania w procesie rekrutacji.

pierwszorzędne znaczenie odgrywają najbardziej podstawowe wartości (ochrona życia i zdrowia, prawa dziecka). Na przykład ochrona prawa do życia i zdrowia czy też ochrona praw dziecka, a z drugiej strony ochrona danych osobowych (autonomii informacyjnej jednostki), chociaż objęte odrębnym reżimem prawnym prawa krajowego, nie mogą stać w sprzeczności z RODO. Ochrona danych osobowych musi służyć w każdej sytuacji jednostce, ale również dobru ogólnospołecznemu, a w konsekwencji też prawidłowemu funkcjonowaniu podmiotów sektora publicznego i prywatnego, do których mają zastosowanie przepisy RODO. Nowy system ochrony danych osobowych na wszystkich poziomach jego wdrażania wymaga przyjęcia sposobów i środków ochrony przemyślanych, proporcjonalnych i adekwatnych do praw objętych ochroną, jak i potencjalnych zagrożeń.

Bibliografia

Banaszak B. (2017), *Prawo konstytucyjne*, 8.wydanie, C.H. Beck, Warszawa.

Dmochowska A., Piotrowska A. (2018), *Ustawa o ochronie danych osobowych*. Komentarz, C.H. Beck, Warszawa.

Czajkowska-Motosiuk K. (2018), *RODO dla samorządu i administracji*, Wyd. Infor, Warszawa.

Czubik A. (2013), *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Instytut Multimedialny, Kraków.

Fajgielski P. (2018), *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych. Komentarz*, Wolters Kluwer, Warszawa.

Gałaj-Emiliańczyk K. (2015), *Ochrona danych osobowych, praktyczny komentarz wzorcowa dokumentacja*, ODDK Spółka z ograniczoną odpowiedzialnością Spółka komandytowa, Gdańsk.

Kawecki M. (2017), *Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Wolters Kluwer, Warszawa;

Krasuski A., Skolimowska D. (2007), *Dane osobowe w przedsiębiorstwie*, LexisNexis, Warszawa.

Krzysztofek M. (2016), *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE)216/679*, Wydawnictwo CH Beck, Warszawa.

Mazur M., *Zgłoszenie naruszeń ochrony danych*, [w:] „ABI EXPERT", nr 3, lipiec-wrzesień 2018;

Młotkiewicz M. *IOD jako punkt kontaktowy*, [w:] „ABI EXPERT", nr 2, kwiecień-czerwiec 2018.

Sobczak J. (2013), *Komentarz do art. 8, Karta Praw Podstawowych Unii Europejskiej. Komentarz*, pod red. Andrzeja Wróbla, Wydawnictwo C.H.Beck,Warszawa.

Stech G. (2019), *Jak się chroni cyberprzestrzeń w Polsce*, [w:]"Computerworld" from IDG, Nr 03/2019, Marzec.

Witkowska-Nowakowska K. (2018), Rozdział I. *Przepisy ogólne*, RODO. *Ogólne rozporządzenie o ochronie danych. Komentarz*, redakcja naukowa E. Bielak-Jomaa, D. Lubasz, Wolters Kluwer, Warszawa.

Źródła prawa powszechnie obowiązującego:

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., (Dz.U. nr 78, z późn.zm.);

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3,5 i 8 oraz uzupełniona Protokołem nr 2, (Dz.U. z 1993 r. nr 61, poz. 284 z późn. zm.);

Karta Praw Podstawowych Unii Europejskiej podpisana w Nicei dnia 7 grudnia 2000 roku (wersja skonsolidowana: Dz.Urz. UE C 202 z 7.06.2016., s. 389);
Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana:Dz.Urz. UE C 202 z 7.06.2016 r., s. 47);
Konwencję nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003 r., poz. 25) zmieniona Protokołem zmieniającym Konwencję sporządzonym w Strasburgu w dniu 10 października 2018 r.
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.Urz. WE L 281/31)*
Ustawa z dnia 23 kwietnia 1964 r. – kodeks cywilny (t.j. Dz.U. z 2018 r. poz.1025 z poźn.zm.).
Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2018 r. poz. 1191 z późn.zm.)
Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2017 r., poz.1318,1524 z późn. zm.)
Ustawa z dnia 5 sierpnia 2010 r.o ochronie informacji niejawnych (t.j. Dz. U. z 2018 r. poz. 412, 650, 1000, 1083, 1669, z 2019 r. poz. 125)
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000)
Ustawa z dnia 5 lipca 2018 r. o krajowy systemie cyberbezpieczeństwa (Dz.U.2018 r., poz. 1560)
Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125)
Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j.: Dz. U. z 2017 r. poz. 2247)

Wyroki sądów i trybunałów

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 27 sierpnia 1997 r. (20837/92)
Wyrok Europejskiego Trybunału Praw Człowieka z dnia 25 listopada 2008 r. (23373/03)
Wyrok Europejskiego Trybunału Praw Człowieka z 27 lutego 2018 r. (66490/09)
Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 15 marca 2017 r. (C- 536/15)
Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 20 grudnia 2017 r. w sprawie (C-434/16)
Wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 r. (sygn. U 3/01)
Wyrok Trybunału Konstytucyjnego z 26 czerwca 2008 r. (sygn.K 8/04)
Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 22 marca 2011 r. (sygn. akt I OSK 623/10)
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 21 września 2005 r. (sygn. akt II SA/Wa 1443/05)
Wyrok Sądu Apelacyjnego w Warszawie z dnia 12 listopada 2013 r., (sygn.akt I ACa 906/13)
Wyroku Sądu Apelacyjnego w Warszawie z dnia 19 maja 2016 r. (sygn. akt I ACa 1056/15)
Sądu Apelacyjnego w Warszawie z dnia 25 listopada2016 r., (sygn. akt I Ca 1565/15)

Inne

„Dziennik Gazeta Prawna", 25-27 maja 2018 TGP nr 19 (124) /DGP nr 101 (4751)
Wytyczne dotyczące inspektorów ochrony danych ('DP') przyjęte w dniu 13 grudnia 2016 r. ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., Grupa Robocza art. 29 ds. Ochrony Danych (http://ec.europa.eu/justice/data-protection/index_en.htm, dostęp 31.03.2019)

Strony internetowe

– www.uodo.gov.pl
– www.gov.pl/cyfryzacja
– www.ec.europa.eu
– www.curia.europa.eu

Dr Katarzyna Chrostowska-Malak, Wydział Administracji i Nauk Społecznych Politechniki Warszawskiej (kchrosto@ans.pw.edu.pl)

Słowa kluczowe: RODO, prawa człowieka, integracja europejska, prawo do prywatności, ochrona prywatności, ochrona danych osobowych

Keywords: GDPR, human rights, European integration, the right to privacy, privacy protection, protection of personal data

ABSTRACT

The provisions of the GDPR in force as of 25.05.2018 form the basis for the creation of a new system for the protection of personal data (protection of the right to privacy) at the EU level, its member states and in individual entities subject to them. Although the Regulation requires compliance to clearly defined rules, it gives the entities to which it applies the possibility to introduce various organizational solutions and means of protection depending on the nature of the organization, its conditions and needs. We have passed the first stage of implementing the new regulations, characterized by uncertainty and information chaos, sometimes accompanied by the fear of high fines. Now, we are entering a phase of greater certainty of action (legal certainty).

Undoubtedly, there is no judicial interpretation of the provisions of the GDPR. On the other hand, the jurisprudence regarding the right to privacy, guidelines of the socalled Working Group, art. 29, and on a regular basis - the guidelines and explanations of state authorities responsible for the implementation of the new EU law prove very helpful. The experience gained, not only in the form of good examples, but also the conclusions drawn from bad practices, referred to as „GDPR absurdities", is becoming more and more valuable.

These situations have made us realize how dangerous it can be to misinterpret law when such an interpretation is done in isolation from the essence of the law. The protection of personal data, although subject to an independent legal regime, is not only a value in itself. It is to serve first and foremost the individual and the social welfare and, consequently, the proper functioning of public and private sector entities to which the provisions of the GDPR apply.

The purpose of this article will be to present the basis of the privacy protection system in the light of the GDPR, and - taking into account less than one year of the functioning of the GDPR - an attempt to formulate proposals that at the current stage seem to be of crucial importance for the process of further development of the personal data protection system.