Rozdział I. Zagadnienia wstępne z zakresu ochrony danych osobowych pracowników

1. Elementarz z zakresu danych osobowych

Krzysztof Kaźmierczak, Paweł Litwiński

1.1. Publicznoprawna ochrona danych osobowych

Jednym z powodów, dla którego ustanowiona została publicznoprawna ochrona danych osobowych, jest pewna praktyczna niedogodność związana z ochroną prywatności tylko na gruncie prawa cywilnego. Ochrona cywilnoprawna możliwa jest bowiem dopiero po stwierdzeniu, że istnieje konkretne zagrożenie dla prywatności – innymi słowy, po naruszeniu prywatności. Stąd ochrona sądowa okazywała się często spóźniona w stosunku do naruszeń, a więc nie mogła tym naruszeniom przeciwdziałać.

Podstawowym założeniem publicznoprawnej ochrony danych osobowych jest wzmocnienie autonomii jednostki w realizacji przysługujących jej praw, w szczególności prawa do prywatności. Odbywa się to za pomocą procedur o charakterze organizacyjnym i za pomocą środków technicznych, a więc za pomocą typowych instrumentów prawa publicznego. Prywatność, czyli dobro z zakresu prawa prywatnego, jest więc chroniona przy pomocy instrumentów prawa publicznego. Doprowadziło to także do powstania pojęcia tzw. **prywatności informacyjnej** – składają się na nią uprawnienia jednostki do kontrolowania treści i obiegu informacji, które jej dotyczą. Na uprawnienia wchodzące w skład prywatności informacyjnej składa się także prawo do poprawiania danych osobowych oraz ich aktualizacji.

Prawo ochrony danych osobowych zalicza się do prawa publicznego, a w polskich realiach tradycyjnie traktowane jest jako element systemu prawa administracyjnego.

Prawo do prywatności jest prawem bezwzględnym, skutecznym wobec wszystkich osób, a na osobach trzecich ciąży obowiązek powstrzymywania się od wszelkich działań, które naruszałyby to prawo. Ochrony takiego prawa nie może ograniczyć bądź wyłączyć oświadczenie osoby, w której prywatność dokonuje się ingerencja – może ona jedynie wy-

razić zgodę na taką ingerencję. Ochrona prawa do prywatności nie zamyka się wyłącznie w granicach cywilnoprawnych środków ochrony tego prawa – w polskim systemie prawnym od 1998 r., a w systemach prawnych innych państw od już dłuższego czasu prawo do prywatności korzysta z ochrony prawa publicznego, realizowanej przy użyciu konstrukcji określanej mianem ochrony danych osobowych.

1.2. Akty prawne regulujące ochronę danych osobowych

Punktem wyjścia dla ustanowienia publicznoprawnej ochrony danych osobowych była dyskusja dotycząca zagrożeń związanych z gromadzeniem informacji o osobach fizycznych, która rozpoczęła się pod koniec lat 50. XX w. w Stanach Zjednoczonych. W skali międzynarodowej za pierwszy akt prawny z dziedziny ochrony danych uznaje się Konwencję Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzoną w Strasburgu 28.1.1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25).

Ustawodawstwo wewnętrzne państw-stron konwencji Nr 108 uchwalone po przyjęciu samej konwencji okazało się bardzo zróżnicowane. Z tego względu w ramach instytucji UE prowadzone były od 1990 r. prace mające na celu opracowanie projektu dyrektywy dotyczącej ochrony danych osobowych. Ich rezultatem stało się przyjęcie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 281 z 23.11.1995 r., s. 31). Dyrektywa jako akt prawa wtórnego UE wiąże państwa członkowskie UE w odniesieniu do rezultatu, który ma być osiągnięty, pozostawiając organom krajowym swobodę wyboru formy i środków stosowanych w tym celu.

W rozdziale II w sekcji I dyrektywy określone zostały podstawowe zasady przetwarzania danych osobowych. Są to:

1) wymóg rzetelnego i zgodnego z prawem przetwarzania danych osobowych, zasada celowości przetwarzania danych,
2) zasada adekwatności przetwarzania danych,
3) zasada poprawności merytorycznej danych,
4) zasada ograniczenia czasowego przetwarzania danych,
5) zasada poszanowania praw osób fizycznych przy przetwarzaniu ich danych osobowych,
6) zasada stosowania odpowiednich środków zabezpieczenia danych,
7) zakaz przekazywania danych poza teren Europejskiego Obszaru Gospodarczego poza przypadkami wskazanymi w dyrektywie.

Dosyć powszechnie za najważniejszą z tych zasad uznaje się wymóg rzetelnego i zgodnego z prawem przetwarzania danych osobowych.

Ważne

W polskim systemie prawnym ochrona danych osobowych wywodzi się z przepisów Konstytucji RP. Artykuł 47 Konstytucji RP gwarantuje każdemu prawo do ochrony życia prywatnego, rodzinnego,

czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W art. 51 Konstytucji RP zawarte zostały bezpośrednie gwarancje ochrony danych osobowych. Należy wśród nich wymienić:

1) prawo do samodzielnego decydowania każdej osoby o ujawnianiu dotyczących jej informacji,
2) prawo każdej osoby do sprawowania kontroli nad informacjami na swój temat, gwarantowane prawem dostępu do dotyczących jej urzędowych dokumentów i zbiorów danych,
3) prawo do weryfikowania lub żądania usunięcia danych osobowych.

W art. 51 ust. 5 Konstytucji RP zawarta została zapowiedź uchwalenia ustawy regulującej „zasady i trybu gromadzenia oraz udostępniania informacji". Wykonaniem tej zapowiedzi stało się uchwalenie OchrDanychU.

1.3. Reforma prawa ochrony danych osobowych

W 2011 r. Komisja Europejska przedstawiła projekt kompleksowej reformy prawa ochrony danych osobowych w UE. Powodem, dla którego podjęto prace nad reformą, był – po pierwsze – upływ ponad 20 lat od czasu, gdy rozpoczęto prace nad dyrektywą 95/46/WE, co spowodowało, że przepisy dyrektywy przestały odpowiadać potrzebom rynku. Po drugie, pomiędzy krajami UE istnieją różnice w sposobie implementowania dyrektywy, co wpływa negatywnie na transgraniczne przetwarzanie danych osobowych. Po trzecie, w dobie globalizacji istnieje potrzeba wprowadzenia zasad współpracy między krajowymi organami ochrony danych osobowych, a takich przepisów dyrektywa nie zawierała. W rezultacie, w 2016 r. ostatecznie przyjęte zostało RODO (tzw. ogólne rozporządzenie o ochronie danych). Rozporządzenie będzie miało zastosowanie od 25.5.2018 r.

Rozporządzenie, inaczej niż dyrektywa, jest aktem prawnym wywołującym bezpośrednie skutki w systemach prawnych państw członkowskich UE. Jednocześnie RODO zawiera całość przepisów prawa materialnego o ochronie danych osobowych, za wyjątkiem pewnych zagadnień, co do których państwa członkowskie UE nie doszły do porozumienia, lub które celowo pozostawiono regulacji poszczególnych państw. Przykładem tego rodzaju kwestii są zasady przetwarzania danych osobowych w kontekście zatrudnienia. Rozporządzenie o ochronie danych zawiera tylko jeden przepis regulujący wprost przetwarzanie danych osobowych pracowników – przepis legalizujący przetwarzanie szczególnych kategorii danych osobowych do celów zatrudnienia, odpowiednik obecnego art. 27 ust. 2 pkt 6 OchrDanychU. Jednocześnie, zgodnie z art. 88 ust. 1 RODO, państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy. Polska może więc przyjąć przepisy krajowe, bardziej szczegółowe niż przepisy RODO, mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrud-

nieniem. Jeżeli więc nie zostaną przyjęte inne szczególne przepisy dotyczące danych pracowników, takie dane będą traktowane na równi z innymi danymi osobowymi.

Pozostałe zagadnienia pozostaną przedmiotem regulacji prawa krajowego – w szczególności kwestie ustrojowe (powołanie i zasady działania organu ochrony danych osobowych), kwestie proceduralne (postępowanie przed GIODO) oraz zapewne przepisy karne. W Polsce trwają obecnie prace nad nową ustawą o ochronie danych osobowych.

Podstawowe zasady prawa ochrony danych osobowych określone zostały w art. 8 RODO. Ich katalog został częściowo rozszerzony w stosunku do tego wynikającego z dyrektywy. Wśród podstawowych zasad prawa ochrony danych osobowych wyróżnić możemy:

1) zasadę przetwarzania zgodnego z prawem, rzetelnego i przejrzystego,
2) zasadę ograniczenia celu zbierania i przetwarzania danych,
3) zasadę minimalizacji danych,
4) zasadę ograniczenia celu przetwarzania danych,
5) zasadę prawidłowości przetwarzania danych,
6) zasadę integralności i poufności przetwarzania,
7) zasadę rozliczalności przetwarzania.

Obok powyższych, RODO wprowadza także zestaw ogólnych zasad, które stosować należy do obowiązków administratora bądź innego podmiotu przetwarzającego w zakresie zabezpieczenia danych i poszanowania praw osoby, której dane dotyczą. Obejmują one:

1) obowiązek oszacowania ryzyka i przeprowadzenia w sytuacjach tego wymagających, analizy ryzyka oraz konsultacji z organem nadzorczym,
2) obowiązek uwzględnienia kwestii związanych z ochroną danych osobowych na etapie projektowania danej czynności.

1.4. Podstawowe pojęcia prawa ochrony danych osobowych

Dla opisania obowiązków związanych z ochroną danych osobowych niezbędne jest wyjaśnienie podstawowych pojęć wykorzystywanych w przepisach.

1.4.1. Pojęcie danych osobowych

Pojęcie danych osobowych ma podstawowe znaczenie dla określenia, do jakich czynności znajdzie zastosowanie RODO oraz OchrDanychU. Definicja tego pojęcia zawarta została w art. 4 pkt 1 RODO oraz art. 6 OchrDanychU; obie te definicje są w dużej mierze jednobrzmiące, wskazując na te same elementy definiujące pojęcie danych osobowych. Zgodnie z treścią definicji RODO, **za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej**. Zatem, aby mówić o danych osobowych, spełnione muszą być jednocześnie trzy elementy:

1) musimy mieć do czynienia z informacjami,
2) informacje te muszą dotyczyć osoby fizycznej,
3) osoba ta musi być zidentyfikowana bądź możliwa do zidentyfikowania.

Ad 1. Wszystkie dane osobowe są przede wszystkim informacjami. Pojęcie to należy interpretować bardzo szeroko, jako każdy rodzaj komunikatu, każdą wiadomość, niezależ-

nie od sposobu jej wyrażenia, zapisania bądź prezentacji. Informacja taka powinna usuwać niepewność co do zaistnienia określonych zdarzeń.

Przykład

Informacjami w rozumieniu art. 4 pkt 1 RODO oraz art. 6 OchrDanychU będą zarówno znaki językowe w formie słownej, jak i pisemnej, obrazy, nagrania, wizerunek, dane biometryczne, cechy źrenicy, linie papilarne, cechy twarzy, geometria ręki i ogólnie wszelkie komunikaty zapisane i pozyskane w jakikolwiek sposób i każde inne dane – o ile tylko zawierają odpowiednią treść, teoretycznie możliwą do odczytania.

Ani ogólne rozporządzenie o ochronie danych, ani OchrDanychU nie wprowadzają wymogów dotyczących treści informacji stanowiących dane osobowe, poza tym, by dotyczyły one osoby. Informacje, by być uznanymi za dane osobowe, nie muszą być zatem prawdziwe, z tym że osoba, której dane dotyczą, będzie miała prawo do żądania sprostowania danych fałszywych, błędnych bądź niekompletnych. Mogą także dotyczyć samych planów osoby, więc okoliczności jeszcze niezrealizowanych – jak np. „Jak Kowalski zamierza wziąć ślub w przyszłym roku", podobnie jak planów osoby trzeciej – np. „Kierownik zamierza dać Janowi Kowalskiemu w przyszłym roku podwyżkę". Mogą także dotyczyć elementów ocen kulturowych, psychologicznych, wyrażonych w związku z jakąś osobą – więc elementów niemożliwych do zweryfikowania.

Ad 2. Zgodnie z drugim elementem definicji, by być uznaną za daną osobową, informacja z art. 4 pkt 1 RODO oraz art. 6 OchrDanychU musi dotyczyć osoby fizycznej. Nie stanowią zatem danych osobowych informacje dotyczące wyłącznie osób prawnych, podmiotów niemających osobowości prawnej, spółdzielni, wspólnot i innych podobnych jednostek organizacyjnych, chyba że w ich treści zawarte będą także informacje dotyczące osób fizycznych. Podobnie nie będą danymi osobowymi dane dotyczące grup osób takich jak przykładowo rodziny czy rody, chyba że mają formę, którą można odnieść do pojedynczych konkretnych członków takiej grupy (np. informacja o występowaniu u członków danej rodziny określonej dziedzicznej choroby genetycznej). Jednocześnie nie będą stanowić danych osobowych informacje dotyczące osób zmarłych – jako że jedynie osoby żyjące w rozumieniu przepisów KC mogą być uznane za osoby fizyczne. Dane osobowe mogą natomiast dotyczyć osoby fizycznej niezależnie od jej wieku czy stanu rozwoju emocjonalnego – więc także dziecka czy osoby ubezwłasnowolnionej.

Od zasady, że danymi osobowymi mogą być tylko dane osoby żyjącej, wyjątkiem są takie dane, które choć dotyczą osób zmarłych, to jednocześnie mogą być odniesione do osób żyjących. W szczególności odnosić się to będzie do danych dotyczących cech czy chorób dziedzicznych, które będzie można powiązać z krewnymi zmarłej osoby. Podobnie wszystkie inne dane, jeżeli z ich natury bądź sposobu zaprezentowania będzie je można połączyć z osobą żyjącą, będą mogły być uznane za dane osobowe – w takiej sytuacji jednak dane takie należy uznać za dane osób żyjących, a nie osoby zmarłej.

Ważne

Wyjątkiem od zasady, że dane powinny dotyczyć osoby fizycznej, jest uznanie za daną osobową danych będących identyfikatorami internetowymi – takich jak adresy IP, identyfikatory plików cookie czy inne podobne identyfikatory generowane w inny sposób. Zasada ta wprowadzona została

pod rządami OchrDanychU w odniesieniu do adresów IP, zaś znajduje potwierdzenie w treści motywu 30 RODO.

Takie identyfikatory mogą być uważane za dane osobowe, jako że pozostawiają pewne ślady, o ile pozwalają ustalić osobę korzystającą z urządzenia bądź aplikacji – czy, jak w przypadku tzw. stałego adresu IP, poprzez pozostawienie pewnych śladów, które ostatecznie mogą być wykorzystane do identyfikacji danej osoby. O tym, czy taki identyfikator będzie uznany za daną osobową, ostatecznie będzie decydowało to, czy jest on przypisany do danej osoby. W szczególności taki charakter może mieć tzw. stały adres IP.

Ad 3. Aby informację dotyczącą osoby fizycznej zaliczyć w poczet danych osobowych, musi ona dotyczyć osoby zidentyfikowanej bądź możliwej do zidentyfikowania. Ogólne rozporządzenie o ochronie danych wskazuje, że taka identyfikacja może być dokonana pośrednio bądź bezpośrednio. Treść tej przesłanki należy rozpatrzyć oddzielnie dla jej obydwu form.

Osobą zidentyfikowaną będzie osoba, którą można wskazać jako bezpośrednio powiązaną z daną informacją, więc wyróżnić ją spośród innych osób na jej podstawie. Dana osobowa będzie w takiej sytuacji pomagała w takim właśnie wyodrębnieniu i będzie przydatna do ustalenia tożsamości takiej osoby. Dla ustalenia, czy informacja dotyczy osoby, którą można zidentyfikować, będzie zatem niezbędne przeprowadzenie dwuczęściowego testu, poprzez sprawdzenie:

1) czy sama informacja pozwala na wyodrębnienie, określenie tożsamości danej osoby. Będzie to możliwe w przypadku niektórych danych, jeżeli same w sobie pozwalają na określenie tożsamości osoby. Przykładem danej, która w każdych okolicznościach będzie daną osobową, jest numer PESEL. Podobnie rzecz ma się z wizerunkiem osoby nagranym za pomocą monitoringu;
2) czy została ona funkcjonalnie powiązana z danymi pozwalającymi wyodrębnić osobę.

W przypadku danych o większym stopniu ogólności niezbędne będzie powiązanie zestawu danych w sposób, który umożliwi określenie osoby, której dotyczą. To, czy taka sytuacja zachodzi, zależeć będzie od specyfiki danej informacji.

Przykład

Zestawienie imienia i nazwiska – jak Jan Nowak – z informacją, że dana osoba zamieszkuje w Krakowie, nie pozwala jeszcze na wyodrębnienie danej osoby i potrzebne byłyby tutaj dalsze, bardziej szczegółowe informacje. Jednocześnie jednak zestawienie tego samego imienia i nazwiska z informacją o miejscu zamieszkania w niewielkiej miejscowości, gdzie mieszka wyłącznie jeden Jan Nowak, mogłoby już być uznane za daną osobową.

Za dane osobowe uznać można także dane osoby, którą można zidentyfikować bezpośrednio bądź pośrednio. Artykuł 4 pkt 1 RODO wskazuje tutaj na katalog danych, które mogą pozwolić na identyfikację osoby – identyfikatorami mogą być przykładowo imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub szczególne czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Motyw 26 preambuły RODO wskazuje dodatkowo, że pojęcie osób możliwych do zidentyfikowania obejmuje takie osoby, które można zidentyfikować, biorąc pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których to sposobów istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej.

To, czy środki mogą być wykorzystane przez osobę możemy ustalić, biorąc pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny, który może sprawić, że osoba stanie się możliwa do zidentyfikowania już po zebraniu danych, gdy administrator będzie miał dostęp do nowych środków przetwarzania. Zatem nie będzie osobą możliwą do zidentyfikowania taka, której identyfikacja wymagałaby nadmiernych kosztów, czasu lub działań, które nie będą dostępne dla administratora. Analizie należy tutaj poddać konkretną sytuację administratora oraz działań, które mógłby podjąć, koszty, które by poniósł – w szczególności, jeżeli ustalenie tożsamości osoby teoretycznie jest możliwe, to czy byłoby ono możliwe przy wykorzystaniu łatwo dostępnych źródeł. W szczególności należy tutaj brać pod uwagę dodatkowe informacje, które określony administrator może posiadać wskutek swojej indywidualnej sytuacji – w tym te, które może zdobyć dzięki środkom prawnym, którymi może dysponować w celu ustalenia tożsamości osoby, której dane dotyczą.

Celem takiego ukształtowania pojęcia danych osobowych jest wyłączenie spod jego zakresu sytuacji, w których ustalenie tożsamości osoby, której dane dotyczą, byłoby możliwe czysto teoretycznie, ale administrator nie mógłby dokonać tego bez wykorzystania nieracjonalnych środków.

W związku z pojęciem osoby możliwej do zidentyfikowania RODO wprowadza pojęcie **pseudonimizacji** danych osobowych. Należy przez to rozumieć pozbawienie informacji o osobie elementów pozwalających na ustalenie jej tożsamości, w taki sposób, że administrator zachowuje możliwość ponownego zidentyfikowania osoby. Z pseudonimizacją będziemy mieli do czynienia np. w sytuacji, w której dane pozwalające na identyfikację osoby zostaną zaszyfrowane, zaś administrator będzie nadal posiadał klucz pozwalający na ponowne odczytanie takich danych.

Ogólne rozporządzenie o ochronie danych wskazuje, że dodatkowe informacje niezbędne do ustalenia tożsamości osoby, której dotyczą dane, powinny być w takiej sytuacji oddzielone poprzez zastosowanie środków technicznych i organizacyjnych, które uniemożliwią ich przypisanie bez usunięcia tych zabezpieczeń. Dane pseudonimizowane pozostaną danymi osobowymi – procedura ta jest natomiast uważana za jedną z metod zabezpieczenia danych osobowych.

Z wymogu, by dane osobowe dotyczyły osoby możliwej do ustalenia, wynika, że nie będą danymi osobowymi takie dane, które zostały **zanonimizowane**, poprzez pozbawienie ich cech pozwalających na powiązanie z osobą, której dotyczą. W szczególności dokonać tego można przez zastąpienie danych identyfikujących (takich jak imiona, nazwiska, miejsce zamieszkania, numery identyfikacyjne, czas dokonania opisanej czynności) symbolami bądź skrótami, które nie pozwolą na odtworzenie treści tak zastąpionego wyraże-

nia. Anonimizację od pseudonomizacji odróżniać będzie trwałość pozbawienia danych możliwości identyfikacji osoby.

1.4.2. Pojęcie szczególnych kategorii danych osobowych

Zarówno RODO, jak i OchrDanychU wyróżniają dwie kategorie danych osobowych. Obok tych, dla których przyjęto określenie danych zwykłych, wyróżnić możemy kategorię danych, o których na gruncie RODO mówimy o szczególnych kategoriach danych osobowych, zaś na gruncie OchrDanychU – o danych wymagających szczególnych zasad ochrony. Często wykorzystywana jest tutaj także nazwa danych wrażliwych bądź danych sensytywnych.

Przetwarzanie takich szczególnych kategorii danych poddane jest dodatkowym wymogom w zakresie ich zbierania, zaś w przypadku OchrDanychU także rejestracji danych.

Katalog szczególnych kategorii danych osobowych zawarty został w art. 9 RODO. Wskazuje on, że do danych objętych szczególnymi zasadami ochrony zaliczyć należy takie dane, które dotyczą:

1) pochodzenia rasowego lub etnicznego,
2) poglądów politycznych,
3) przekonań religijnych lub światopoglądowych,
4) przynależności do związków zawodowych
5) danych genetycznych,
6) danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej,
7) danych dotyczących zdrowia,
8) danych dotyczących seksualności lub orientacji seksualnej tej osoby.

Katalog danych wrażliwych w RODO jest częściowo odmienny od tego określonego w art. 27 ust. 1 OchrDanychU. Wskazuje on, że do danych objętych szczególnymi zasadami ochrony należą wszelkie takie dane, które dotyczą:

1) pochodzenia rasowego bądź etnicznego,
2) poglądów politycznych,
3) przekonań religijnych lub filozoficznych,
4) przynależności wyznaniowej, partyjnej lub związkowej,
5) danych o stanie zdrowia,
6) danych o kodzie genetycznym,
7) danych o nałogach i życiu seksualnym,
8) skazań, orzeczeń o ukaraniu i mandatów karnych.

Porównując obydwa te katalogi danych, widać, że RODO w miejsce danych dotyczących przekonań filozoficznych, chronionych na gruncie OchrDanychU, wprowadza kategorię danych dotyczących przekonań światopoglądowych – jest to istotne ograniczenie zakresu danych objętych specjalnymi zasadami ochrony jedynie do przekonań osoby o fundamentalnym dla niej znaczeniu.

Ogólne rozporządzenie o ochronie danych nie wskazuje na oddzielne kategorie danych dotyczących przynależności wyznaniowej, partyjnej bądź związkowej. Dane te jednak

pozostaną, co do zasady, objęte specjalnymi zasadami ochrony w tym zakresie, w jakim ujawniają przekonania religijne i światopoglądowe osoby, której dotyczą.

W miejsce niejasnego pojęcia danych o kodzie genetycznym RODO wskazuje jednolitą kategorię danych genetycznych, które rozumieć należy zgodnie z definicją art. 4 pkt 13 RODO, jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają m.in. z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

Ogólne rozporządzenie o ochronie danych wprowadza nieznane w OchrDanychU, choć często wcześniej wykorzystywane pojęcie danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej jako danych objętych specjalnymi zasadami ochrony. Definicja takich danych zawarta została w art. 4 pkt 14 RODO i zawiera trzy elementy, które powinny być spełnione łącznie. Danymi biometrycznymi są takie dane osobowe, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej. Dane te powinny być rezultatem specjalnego przetwarzania przy wykorzystaniu środków technicznych, pozwalających na zebranie takich danych, przetworzenie ich za pomocą algorytmu w matematyczną reprezentację takiej cechy. Dane te powinny być następnie przetwarzane w konkretnym celu, którym jest bądź określenie tożsamości jednostki, bądź potwierdzenie tożsamości ustalonej w inny sposób. Danymi biometrycznymi w szczególności mogą być wizerunek twarzy lub dane daktyloskopijne – o ile tylko są przetwarzane we wskazanym powyżej celu.

Ogólne rozporządzenie o ochronie danych odchodzi od oddzielnego wskazania danych o nałogach jako danych sensytywnych. Dane te jednak pozostaną objęte szczególnymi zasadami ochrony, o ile będzie je można uznać za dane o stanie zdrowia – dotyczyć to będzie zwłaszcza form uzależnienia rozpoznanych jako zespoły uzależnień[1].

Ogólne rozporządzenie o ochronie danych w przeciwieństwie do OchrDanychU nie wskazuje wśród danych wrażliwych kategorii danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych. Dane takie zatem po wejściu w życie nowych przepisów nie będą uważane za wrażliwe – natomiast przed tym dniem nadal trzeba będzie je poddać specjalnym zasadom ochrony. Podkreślić jednak należy, że szczególne zasady przetwarzania takich danych mogą zostać przyjęte przez państwa członkowskie na zasadzie art. 10 RODO.

Katalog danych objętych szczególnymi zasadami ochrony jest zamknięty – a więc żadne inne dane poza wymienionymi w przepisach nie mogą być uznane za takie dane. Dane objęte szczególnymi zasadami ochrony wyodrębnione zostały ze względu na szczególne znaczenie, jakie mają dla osoby, której dotyczą, jako dotykające sfer należących bezpośrednio do stref intymności. Nie ma przeszkody, by informacja należała do więcej niż jednej kategorii danych osobowych – tak więc przykładowo dane dotyczące przekonań religijnych mogą być jednocześnie danymi o przekonaniach światopoglądowych, zaś dane genetyczne będą często jednocześnie danymi o stanie zdrowia.

[1] W szczególności dotyczy to danych o uzależnieniu od alkoholu, opiatów, kanabinoli, substancji nasennych i uspokajających, kokainy, innych niż kokaina środków pobudzających, halucynogenów, tytoniu, odurzania się lotnymi rozpuszczalnikami organicznymi oraz naprzemiennego zażywania takich środków.

1.4.3. Pojęcie administratora danych osobowych

Spośród adresatów przepisów o ochronie danych osobowych szczególne znaczenie należy przypisać administratorowi danych. Jest on w najszerszym stopniu upoważniony do przetwarzania danych i równocześnie ponosi największą odpowiedzialność za zgodność przetwarzania z przepisami. Pojęcie administratora zdefiniowane zostało w art. 4 pkt 7 RODO. Zgodnie z treścią tego przepisu, administratorem danych może być:

1) osoba fizyczna bądź prawna,
2) organ publiczny,
3) jakikolwiek inny podmiot.

W OchrDanychU definicja administratora danych zawarta została w art. 7 pkt 4. Zawiera ona rozwiązanie analogiczne do istniejącego na gruncie RODO, wskazując jedynie szerszy katalog podmiotów przykładowo mogących być administratorami – obejmujący osoby fizyczne lub prawne, jednostki organizacyjne niemające zdolności prawnej, organy państwowe i samorządowe, państwowe i komunalne jednostki organizacyjne oraz jakikolwiek inny podmiot. Żaden z tych katalogów, ani w RODO, ani w OchrDanychU, nie ma charakteru wyczerpującego, a jedynie przykładowy.

Uznanie jednostki organizacyjnej za administratora danych jest niezależne od posiadania przez nią jakiejkolwiek formy organizacyjnej, w szczególności od posiadania przez administratora osobowości prawnej. Administratorem może być podmiot niezależnie od swojego charakteru prawnego, o ile tylko jest w stanie wykonywać funkcje, które decydują o przyznaniu mu statusu administratora opisane w dalszej części przepisu. Nie ma tutaj także znaczenia to, czy dany podmiot obciążają koszty przetwarzania danych osobowych.

Dla uznania za administratora danych decydujące znaczenie będzie miało spełnienie przez podmiot dwóch kryteriów dotyczących sposobów działania wymienionych w dalszej części przepisu. Podmiot taki powinien:

1) decydować o celach przetwarzania danych osobowych,
2) decydować o środkach przetwarzania danych osobowych.

Ad 1. Administratorem jest podmiot, który podejmuje decyzję o celach przetwarzania danych – czyli przetwarza je w celu przez siebie wyznaczonym, zarówno jeżeli jest to jego działalność podstawowa, jak i uboczna, związana z innymi czynnościami. Nie ma tutaj znaczenia, czy dany podmiot jest zobowiązany do przetwarzania danych na podstawie przepisu ustawy – w takiej sytuacji dane są przetwarzane przez administratora we własnym celu, którym jest m.in. wypełnienie ciążącego na nim obowiązku prawnego. Nie ma także znaczenia to, czy przetwarzanie danych związane jest z działalnością zarobkową takiego podmiotu. Podstawowym wyznacznikiem tego, czy podmiot wykorzystuje dane we własnym celu, będzie to, czy podjął decyzję o zebraniu danych oraz o wykonywaniu aktywności, do której będą one wykorzystywane. Tak więc np. w przypadku zbierania danych osobowych pracowników pracodawca podejmuje decyzję o celu przetwarzania danych – w tym przypadku o zatrudnieniu pracowników.

W przypadku trudności z ustaleniem, który podmiot decyduje o celu przetwarzania danych w związku z istnieniem powiązań pomiędzy grupą podmiotów, należy przeanalizo-

wać, kto dane w określonym zakresie by przetwarzał, gdyby takich powiązań nie było – a więc który podmiot działa w sposób wymagający danych osobowych i który podjął decyzję o wykonywaniu takiej działalności. W większości przypadków ten właśnie podmiot zazwyczaj będzie decydował o celu przetwarzania. W reżimie RODO możliwa jest tutaj także sytuacja, w której mamy do czynienia ze współadministratorami danych.

Ad 2. Drugą z przesłanek uznania za administratora danych jest decydowanie o środkach przetwarzania danych. Oznacza to, że podmiot podejmuje decyzję co do tego, jakie formy przyjmie przetwarzanie danych, jakie środki zastosowane będą do ich przetwarzania – w szczególności o tym, jakie dane będą przetwarzane przy wykorzystaniu systemów komputerowych, a jakie przy wykorzystaniu środków tradycyjnych, jakie osoby w jakim zakresie będą upoważnione do przetwarzania danych w imieniu administratora, jakie środki będą stosowane do ochrony takich danych. Również i w tym zakresie nie będzie miało znaczenia to, czy przepisy prawa nakładają na dany podmiot obowiązek określonego zachowania i przetwarzania, gdyż w takiej sytuacji administrator będzie podejmował decyzję o środkach przetwarzania danych, decydując się przetwarzać je w taki sposób, by wypełnić nałożony nań przez przepisy obowiązek określonego zachowania.

Dla uznania za administratora danych nie będzie miało znaczenia to, czy dany podmiot rzeczywiście danymi dysponuje. Dopuszczalna jest sytuacja, w której administrator danych powierza wykonywanie wszystkich czynności na danych innym podmiotom na podstawie umów powierzenia danych, nie tracąc przy tym statusu administratora, o ile tylko podejmuje samodzielnie decyzje dotyczące celów i środków przetwarzania. W takiej sytuacji administrator podejmuje decyzję o zawarciu z innymi podmiotami umów powierzenia dotyczących danych i w ten sposób decyduje o środkach przetwarzania danych, zaś dane te są wciąż przetwarzane w jego celach przez inne podmioty. Nawet jeżeli taka umowa nie zobowiązuje podmiotu, który danymi faktycznie będzie dysponował, do stosowania konkretnych środków przetwarzania danych, to administrator postanawia o przekazaniu decyzyjności w tym zakresie innemu podmiotowi i w ten sposób decyduje o środkach przetwarzania danych.

Status administratora każdy podmiot będzie miał niezależnie dla różnych zbiorów czy zestawów danych osobowych. Powszechnie spotykaną sytuacją jest taka, w której podmiot jest administratorem danych osobowych dla określonych zestawów danych, podczas gdy nie ma takiego statusu dla innych zbiorów danych, którymi dysponuje na innej zasadzie.

To sam podmiot, w imieniu którego przetwarzane są dane osobowe, będzie administratorem danych. W szczególności, nie będzie nim np. osoba podejmująca w przedsiębiorstwie decyzje dotyczące przetwarzania danych, czy to wskutek pełnienia przez siebie funkcji kierowniczej, czy wskutek wyznaczenia do wykonywania zadań związanych z ochroną i operacjami na danych osobowych. Osoby takie będą jedynie wykonywały swoje zadania w imieniu administratora, mogą być określone jako „administrujący" danymi osobowymi.

Ważne

W stosunkach zatrudnienia, co do zasady, to pracodawca jest administratorem danych osobowych zebranych w związku z zatrudnieniem, niezależnie od jego formy – więc osób zatrudnionych na podstawie umowy o pracę czy osób wykonujących czynności na podstawie umów cywilnopraw-

nych, bez względu na to, czy dane takie zostały powierzone innemu podmiotowi, np. w celu prowadzenia księgowości, obsługi płacowo-kadrowej czy sprawdzenia prawdziwości wskazanych przez pracownika w życiorysie informacji. Podobnie to pracodawca będzie administratorem danych osobowych innych osób zebranych w związku z zatrudnieniem, jak np. danych członków rodzin pracownika, zebranych w związku ze świadczeniami socjalnymi, z których korzystają pracownicy, specjalnymi uprawnieniami związanymi z posiadaniem przez pracownika dzieci czy danych osoby, którą pracodawca ma powiadomić w razie wypadku pracownika.

Wyjątkiem będzie tutaj zatrudnienie w warunkach pracy tymczasowej. W takiej sytuacji, jak wynika z uregulowań ustawowych zawartych w ZatrPracTymczU, to agencja zatrudnia pracownika na podstawie umowy o pracę, w celu delegowania go do zakładu, który następnie z pracy takiej osoby korzysta i ją nadzoruje. Wobec tego to agencja pracy tymczasowej będzie decydowała o celu i sposobie przetwarzania danych, tj. decydując o zatrudnieniu pracownika tymczasowego oraz o metodach ich przetwarzania i zabezpieczenia. Zatem to agencja, a nie zakład, w którym pracownik wykonuje pracę, będzie administratorem danych zebranych w związku z zatrudnieniem.

W przypadku podmiotów zajmujących się pośrednictwem pomiędzy pracodawcą a osobami poszukującymi pracy, to, jak będzie kształtował się status podmiotów, zależeć będzie od formy działalności takiego zakładu. Jeżeli podmiot taki zajmuje się pośrednictwem przy ogłaszaniu ofert pracodawców i przesyła im aplikacje osób szukających pracy, wówczas to pracodawca pozostaje administratorem danych, zaś podmiot zajmujący się pośrednictwem będzie operował na danych na podstawie umowy powierzenia. Natomiast, jeżeli podmiot taki we własnym zakresie gromadzi dane osób bez bezpośredniego związku z konkretną ofertą, a następnie na pytanie potencjalnego pracodawcy o kandydatów przesyła aplikacje tych, które odpowiadają poszukiwanym pracownikom, to wówczas będziemy mogli mówić o dwóch administratorach danych. Pierwszy będzie podmiot pośredniczący, który będzie administratorem danych osób poszukujących pracy, zaś drugim – potencjalny pracodawca, przetwarzający dane w celu rekrutacji.

Ogólne rozporządzenie o ochronie danych wprowadza dodatkowe rozwiązanie, bezpośrednio powiązane z pojęciem administratora danych – **współadministratorów danych**. Zgodnie z definicją administratora danych, może bowiem decydować o zasadach przetwarzania danych wspólnie w innym podmiotem – w takiej sytuacji mamy do czynienia ze współadministratorami danych.

Pojęcie współadministratorów danych zostało zdefiniowane w art. 26 RODO. Zgodnie z tym pojęciem, o współadministratorach mówimy wówczas, gdy dwa lub więcej podmiotów wspólnie ustala cele i środki przetwarzania danych osobowych. Dotyczyć to będzie zatem w szczególności takich przypadków, w których np. określona platforma komputerowa jest wykorzystywana przez więcej niż jeden podmiot w tych samych celach, którą to platformą obydwa podmioty razem administrują i zarządzają. Ze współadministratorami często będziemy mieli także do czynienia w takich sytuacjach, gdy kilka spółek należy do określonej grupy i korzystają z tego samego zbioru danych, każda dla swojego celu, czy gdy kilka podmiotów powołało wspólny komitet decydujący o zasadach przetwarzania danych.

W przypadku gdy podmioty działają jako współadministratorzy, art. 26 RODO nakłada na nie obowiązek określenia w sposób przejrzysty i jasny zakresów swojej odpowiedzialności za wypełnienie wymogów dotyczących danych. Takie uzgodnienia dokonane pomiędzy podmiotami powinny należycie odzwierciedlać wzajemne obowiązki i funkcje

stron w stosunku do danych oraz ich relacje z osobami, których dane dotyczą, zaś podstawowe elementy tak dokonanych uzgodnień powinny być ujawnione takim osobom. Niezależnie od treści takich uzgodnień, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wobec każdego ze współadministratorów.

Dokonanie uzgodnień nie jest niezbędne, gdy wzajemne relacje i obowiązki administratorów wynikają z przepisów prawa, z tym że strony mogą wskazać jeden punkt kontaktowy dla osób, których dane dotyczą.

1.4.4. Pojęcie przetwarzania danych

Pojęcie przetwarzania danych ma decydujące znaczenie dla tego, jakie czynności objęte są obowiązkami wynikającymi zarówno z RODO, jak i z OchrDanychU. Regulacje tych aktów prawnych dotyczą przede wszystkim właśnie zasad i ochrony przetwarzania danych.

Definicja przetwarzania danych jest zawarta w art. 4 pkt 2 RODO. Zgodnie z jego treścią, pod tym pojęciem należy rozumieć jakiekolwiek operacje wykonywane na danych osobowych.

Zakres pojęcia przetwarzania danych jest bardzo szeroki i dotyczy wszelkiego rodzaju działań dokonywanych na danych – w szczególności nie obejmuje ono, jak wskazywałoby dosłowne rozumienie pojęcia „przetwarzanie", jedynie operacji skutkujących transformacją, zmianą treści danych. Nie ma także znaczenia, czy działania te są podejmowane w sposób zautomatyzowany czy też niezautomatyzowany, obydwie te formy w równym stopniu będą mogły stanowić przetwarzanie danych.

Zawarta w RODO definicja pojęcia przetwarzania danych wskazuje dalej na przykładowy zestaw operacji, które są uważane za przetwarzanie danych. Katalog ten nie jest w żaden sposób wyczerpujący, a jedynie zawiera wyliczenie czynności, które niewątpliwie należy uznać za przetwarzanie danych. Katalog ten obejmuje:

1) zbieranie danych – uzyskiwanie ich w jakikolwiek sposób, bez względu na to, czy ostatecznie zostaną one zapisane czy usunięte;
2) utrwalanie danych – zapisanie ich na jakimkolwiek materialnym nośniku;
3) organizowanie danych – łączenie i dopasowywanie danych;
4) porządkowanie danych – układanie nośników danych według określonego kryterium;
5) przechowywanie danych – sam akt posiadania i przechowywania danych, choćby bez dostępu do ich treści, stanowi jedną z form przetwarzania danych. Dotyczy to nawet sytuacji, w której podmiot przechowujący dane nie będzie miał w danym momencie środków technicznych do zapoznania się z ich treścią. Więc np. w sytuacji, w której przechowywane są dane zaszyfrowane, zaś podmiot przechowujący nie będzie miał możliwości ich odczytania, wciąż będzie on przetwarzał dane;
6) adaptowanie lub modyfikowanie danych – każde zmienianie formatu i metody, w jakiej dane są zapisane, oraz ingerowanie w ich treść;
7) pobieranie danych – pozyskiwanie i zapisywanie danych ze źródeł ogólnodostępnych;

8) przeglądanie danych – zapoznawanie się z treścią i zawartością zestawów danych osobowych;
9) wykorzystywanie danych – dokonywanie każdej czynności, dla której potrzebne jest wykorzystanie danych osobowych;
10) ujawnianie danych poprzez przesłanie – przekazanie danych do pojedynczego, konkretnego odbiorcy;
11) rozpowszechnianie lub innego rodzaju udostępnianie danych – umożliwienie dostępu do danych dla otwartej grupy odbiorców, np. poprzez umieszczenie danych w publicznie dostępnym miejscu;
12) dopasowywanie lub łączenie danych – tworzenie powiązań pomiędzy różnymi zestawami danych osobowych;
13) ograniczanie danych – częściowe usunięcie danych, pozbawienie ich pewnych połączeń i powiązań z innymi danymi;
14) usuwanie danych – pozbawienie danych własności pozwalających na uznanie ich za dane osobowe;
15) niszczenie danych – trwałe wykasowanie danych, poprzez całkowite usunięcie ich z nośnika, na którym zostały utrwalone.

Definicja przetwarzania danych zawarta w RODO jest analogiczna do tej zawartej w art. 7 pkt 2 OchrDanychU. Jedyną różnicą jest wskazanie w OchrDanychU krótszego katalogu przykładowych operacji będących przetwarzaniem, obejmującego zbieranie danych, ich utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. W obydwu przypadkach katalogi te należy uznać za przykładowe i niewykluczające uznania innych operacji na danych za będące ich przetwarzaniem. Zatem **czynności, które będzie należało uznać za przetwarzanie danych na gruncie OchrDanychU, pozostaną takimi po rozpoczęciu stosowania RODO**.

Ważne

Z przetwarzaniem danych będziemy mogli mieć do czynienia na każdym dotyczącym ich etapie działań – zarówno podczas ich zbierania, jak i w momencie ich zgromadzenia, a także później – w trakcie jakiegokolwiek ich wykorzystywania, niezależnie od formy takiego wykorzystania, oraz po ich wykorzystaniu w momencie usunięcia. Z każdym etapem takiej działalności będą łączyły się obowiązki, które RODO oraz OchrDanychU wiążą z przetwarzaniem.

1.4.5. Pojęcie zbioru danych

Pojęcie zbioru danych ma zasadnicze znaczenie dla określenia takich obowiązków związanych z przetwarzaniem danych osobowych, które dotyczą jedynie danych przetwarzanych w zbiorach. Definicja zbioru danych osobowych zawarta jest w art. 4 pkt 6 RODO. Zgodnie z treścią tego przepisu, aby można było mówić o zbiorze, niezbędne jest łączne wypełnienie dwóch warunków:
1) musi to być zestaw danych o charakterze osobowym,
2) zbiór taki musi być uporządkowany, zaś dane w nim zawarte muszą być dostępne według określonego kryterium.

Podobną definicję zawiera art. 7 pkt 1 OchrDanychU, który wskazuje, że zbiorem danych jest każdy mający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów. Funkcjonalnie te dwie definicje wydają się tożsame.

Ad 1. By mówić o zbiorze, musimy mieć do czynienia z zestawieniem pewnej liczby danych. Niezbędna jest zatem taka ilość informacji, by mogły one tworzyć zestaw, natomiast ani RODO, ani też OchrDanychU nie wprowadzają żadnego dookreślenia tego, ile takich elementów powinno być. Brak jest także wymogów dotyczących tego, by dane zawarte w zbiorze dotyczyły określonej minimalnie liczby osób. Już niewielki zestaw danych będzie mógł spełnić wymóg bycia zestawem, nawet jeżeli jest to jedynie zestawienie pewnej liczby danych dotyczących pojedynczej osoby.

Ad 2. Drugą z ustawowych przesłanek jest posiadanie przez zbiór struktury takiej, by dane te były uporządkowane i dostępne według określonego kryterium. Wyłącza to z ustawowego pojęcia zestawy danych nieuporządkowanych, ułożonych zupełnie przypadkowo. Druga część tego wymogu wskazuje na sposób takiego ułożenia – dane muszą być dostępne według określonego kryterium. Należy przez to rozumieć taki sposób zorganizowania i dostępu do danych, by możliwe było wyszukanie konkretnego rekordu w sposób niebędący przypadkowym i niewymagający analizy dużej części zestawu danych. Kryterium, według którego dane będą dostępne, powinno być zatem jedną z cech, fragmentem rekordu danych mającym znaczenie dla podmiotu wyszukującego dane w określonym zbiorze, w szczególności dla administratora danych.

Dla uznania zestawienia danych za zbiór nie będzie miało znaczenia to, czy jest on przetwarzany w formie tradycyjnej, czy też został zapisany w systemie informatycznym. Zbiór danych osobowych nie musi być także fizycznie ulokowany w tym samym miejscu. W dalszej części art. 4 pkt 2 RODO wskazuje, że dla uznania zestawu danych za zbiór nie ma znaczenia to, czy jego elementy są rozproszone geograficznie. Ważne jest tylko, by elementy tego zbioru były uporządkowane i dostępne według tego samego kryterium, niezależnie od ich wzajemnego położenia. Tak więc np. zbiór danych pracowniczych, choćby ulokowany ze względów praktycznych w różnych oddziałach spółki, dostępny według kryterium miejsca wykonywania pracy i danych samego pracownika, pozostanie jednym zbiorem danych.

Przykład

Przykładowymi typami zbiorów danych osobowych, które zazwyczaj można znaleźć w większości przedsiębiorstw, mogą być:

1) zbiór danych pracowników – obejmujący dane zebrane w związku z zatrudnieniem, w tym zwłaszcza dane kadrowo-płacowe,
2) zbiór danych kandydatów do pracy – obejmujący dane osób ubiegających się o przyjęcie na stanowisko,
3) zbiór danych klientów i współpracowników – obejmujący dane osób, z którymi przedsiębiorstwo współpracowało w jakiejś formie,
4) zbiór danych osób odwiedzających przedsiębiorstwo – zawarty np. w księdze gości.