Received: 14.09.2021
Accepted: 16.11.2021
Published: 31.12.2021

Roczniki Administracji i Prawa
Annuals of The Administration and Law
2021, XXI, z. 4: s. 223-246
ISSN: 1644-9126
DOI: 10.5604/01.3001.0015.8313
https://rocznikiadministracjiiprawa.publisherspanel.com

Dominika Dörre-Kolasa*
Nr ORCID: 0000-0002-4134-741X

Marlena Sakowska-Baryła**
Nr ORCID: 0000-0002-3982-976X

O KASACH ZAPOMOGOWO-POŻYCZKOWYCH W ŚWIETLE ZASAD OCHRONY DANYCH OSOBOWYCH

ABOUT CREDIT UNIONS IN LIGHT OF PERSONAL DATA PROTECTION PRINCIPLES

Streszczenie: Od 11 października 2021 r. zasady tworzenia, organizowania i działania u pracodawcy pracowniczej kasy zapomogowo-pożyczkowej (dalej: KZP) określa nowa ustawa z dnia 11 sierpnia 2021 r. o kasach zapomogowo-pożyczkowych (dalej: uKZP). Warto przyjrzeć się jej przepisom pod kątem wpływu, jaki może mieć na przetwarzanie danych osobowych. Ustawodawca w ustawie o kasach zapomogowo-pożyczkowych przetwarzaniu danych osobowych poświęca art. 43. Nie jest to jednak jedyny przepis odnoszący się do kwestii danych osobowych. Regulacje zawarte w tej ustawie – jak się wydaje – miały przeciąć m.in. liczne dywagacje dotyczące przetwarzania danych osobowych przez podmioty tego rodzaju. Lektura tych przepisów nie w każdym przypadku pozwala jednak na tak pozytywne wnioski.

Słowa kluczowe: kasa zapomogowo-pożyczkowa, dane osobowe, pracodawca, administrator danych osobnych, przetwarzanie danych

Summary: As of 11 October 2021, the rules of establishing, organizing and operating an employee welfare and loan fund (hereinafter: KZP) at an employer's company are set out in the new Act on Welfare and Loan Funds of 11 August 2021 . It is worth examining its provisions in terms of the impact it may have on the processing of personal data. The legislator devotes Article 43 to the processing of personal data. However, this is not the only provision referring to personal data. It seems that the regulations included in the Act were meant to cut through, among others, numerous discussions

* dr; adiunkt w Katedrze Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego, radca prawny, partner w kancelarii prawa HR. Źródła finansowania publikacji: środki własne autorki, e-mail: dominika.dorre-nowak@uj.edu.pl

** dr; radca prawny, partner w Sakowska-Baryła, Czaplińska Kancelarii Radców Prawnych Sp.p., redaktor naczelna „ABI Expert", członkini kadry naukowej Instytutu Prawa Nowych Technologii i Ochrony Danych Osobowych na Uczelni Łazarskiego. Źródła finansowania publikacji: środki własne autorki. e-mail: m.sakowska-baryla@kancelariasbc.pl

on personal data processing by such entities. Reading these regulations, however, does not in every case allow for such positive conclusions.

Keywords: loan and credit fund, personal data, employer, employer, personal data controller, data processing

WPROWADZENIE

Od dnia 11 października 2021 r. zasady tworzenia, organizowania i działania u pracodawców kas zapomogowo-pożyczkowych, określa ustawa z dnia 11 sierpnia 2021 r. o kasach zapomogowo-pożyczkowych (Dz.U. poz. 1666) – dalej: „ustawa o KZP". Kasy zapomogowo-pożyczkowe funkcjonowały w polskim porządku prawnym od dawna, z tą jednak różnicą, iż obecnie ustawodawca zdecydował się na wprowadzenie autonomicznej i całościowej regulacji ustawowej dla kas zapomogowo-pożyczkowych. Wartościowe dla przeprowadzenia analizy funkcjonowania kas zapomogowo-pożyczkowych wydaje się być przedstawienie, przynajmniej w zarysie, ich ewolucji organizacyjno-prawnej. Wiele rozwiązań pozostało niezmienionych, a zatem może okazać się to przydatne dla właściwego zrozumienia istoty i zasad funkcjonowania kas zapomogowo-pożyczkowych zwłaszcza wówczas, gdy uwzględnimy procesy przetwarzania danych, jakie przy tej okazji zachodzą.

Niniejsze opracowanie ma charakter wprowadzający. Ilość szczegółowych zagadnień, w ramach zdiagnozowanych powiązań podmiotowych, którym towarzyszą przepływy danych osobowych, wymaga kontynuacji w kolejnych opracowaniach, jakie pojawią się w związku z pogłębioną analizą przepisów ustawy.

ZARYS HISTORYCZNY

Jeszcze przed wejściem w życie poprzedniej ustawy o związkach zawodowych, tj. ustawy z dnia 8 października 1982 r. o związkach zawodowych[1], status prawny kas zapomogowo-pożyczkowych był regulowany uchwałą Centralnej Rady Związków Zawodowych z dnia 24 maja 1973 r. w sprawie dalszego rozwoju pracowniczych kas zapomogowo-pożyczkowych i zmian w ramowym regulaminie PKZP[2]. Uchwała ta ustalała Ramowy regulamin PKZP, na podstawie którego opracowywane były regulaminy poszczególnych kas działających w zakładach pracy. W regulaminie tym wyraźnie stwierdzono, że PKZP jest agendą związku zawodowego i kieruje się w swojej działalności przepisami statutu związku zawodowego. Kasy zapomogowo-pożyczkowe stanowiły wówczas element (tzw. agendę) struktury organizacyjnej związku zawodowego jako osoby prawnej[3]. Pracownik przyjęty w poczet członków pracowniczej kasy zapomogowo-pożyczkowej był obowiązany wpłacić wpisowe w wysokości 1% sumy miesięcznego zarobku brutto i wpłacać miesięczny wkład członkowski na fundusz oszczędnościowo-pożyczkowy w wysokości ustalonej w regulaminie kasy. W zamian za to mógł korzystać z pożyczek oraz

[1] Dz.U. nr 32, poz. 16, ze zm.
[2] Biuletyn CRZZ z 1973 r., nr 8, poz. 438
[3] Uzasadnienie uchwały siedmiu sędziów Sądu Najwyższego z dnia 22 grudnia 1979 r., III CZP 27/79, OSNC 1980, z. 4, poz. 64.

z innych form pomocy prowadzonych przez kasę. Kasy zapomogowo-pożyczkowe, działając na zasadach społecznych i „samopomocowych", były postrzegane jako istotne odciążenie środków państwowych kierowanych na udzielenie kredytu pracownikom zakładów pracy. Bezpośrednim ich celem było propagowanie oszczędności i gospodarności, udzielanie członkom pomocy materialnej, wychowywanie członków w duchu koleżeństwa, niesienia wzajemnej pomocy i ponoszenia solidarnej odpowiedzialności[4].

W późniejszym okresie nastąpiła istotna ewolucja w zakresie prawno-organizacyjnego statusu pracowniczych kas zapomogowo-pożyczkowych polegająca na ich wyodrębnieniu ze struktury związków zawodowych. Kasy przestały być agendami związkowymi, a przynależność związkowa przestała mieć znaczenie dla uzyskania statusu członka kasy. Na podstawie art. 51 ust. 1 ustawy z 1982 r. o związkach zawodowych kasy zostały poddane „nadzorowi społecznemu związków zawodowych". Ogólny zapis w ustawie o związkach zawodowych uzupełniało zarządzenie Ministra Pracy, Płac i Spraw Socjalnych z dnia 21 maja 1983 r. w sprawie zasad organizowania i funkcjonowania pracowniczych kas zapomogowo-pożyczkowych w uspołecznionych zakładach pracy oraz obowiązków tych zakładów wobec pracowniczych kas zapomogowo-pożyczkowych[5].

Koncepcja niezależnych organizacyjnie od związków zawodowych kas zapomogowo-pożyczkowych została następnie utrzymana w przepisach ustawy o związkach zawodowych z dnia 23 maja 1991 r. i wydanego na jej podstawie rozporządzenia Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy[6]. Na podstawie art. 39 ustawy o związkach zawodowych – uchylonego wraz z wejściem w życie ustawy z dnia 11 sierpnia 2021 r. o kasach zapomogowo-pożyczkowych – w zakładach pracy mogły być tworzone pracownicze kasy zapomogowo-pożyczkowe, których członkami mogli być pracownicy, emeryci i renciści bez względu na ich przynależność związkową. Dla związków zawodowych przewidziany był „nadzór społeczny nad kasami", co wynikało wprost z ust. 2 art. 39 ustawy o związkach zawodowych.

W obowiązującej od 11 października 2021 r. ustawie o kasach zapomogowo-pożyczkowych „społeczny nadzór" został zastąpiony „kontrolą". Warte podkreślenia jest to, iż nie został przełamany monopol związkowy w tym zakresie. Jak wynika z art. 5 ustawy o KZP, kontrolę nad KZP sprawuje co do zasady działająca u pracodawcy zakładowa organizacja związkowa, o której mowa w art. 25^1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych. Dopiero jeżeli u pracodawcy nie działa zakładowa organizacja związkowa, kontrolę nad KZP sprawuje rada pracowników, o której mowa w ustawie z dnia 7 kwietnia 2006 r. o informowaniu pracowników i przeprowadzaniu z nimi konsultacji (Dz.U. poz. 550, z 2008 r., poz. 584 i 778 oraz z 2009 r., poz. 805). Wówczas, gdy nie działa rada pracowników, kontrolę nad KZP sprawuje reprezentacja osób wykonujących pracę zarobkową wyłoniona w trybie przyjętym u danego pracodawcy.

Owa kontrola nie została, jak się wydaje, przez ustawodawcę dostrzeżona i właściwie umiejscowiona w ramach regulacji dotyczącej ochrony danych osobowych, na co wskazują chociażby przewidziane w ustawie wyłącznie dla kasy ustawowe okresy przetwarzania danych, o czym będzie mowa w dalszej części opracowania.

[4] Uchwała SN(7z) z 22 grudnia 1979 r., III CZP 27/79, OSNC 1980, nr 4, poz. 64.
[5] M.P. nr 19, poz. 110, ze zm.
[6] Dz.U. nr 110, poz. 502, ze zm.

REGULACJE Z ZAKRESU DANYCH OSOBOWYCH

W ustawie o KZP uregulowane zostały niektóre zagadnienia z zakresu ochrony danych osobowych. Z jednej strony zainteresowanie ustawodawcy tą właśnie problematyką wydaje się działaniem uzasadnionym, zważywszy na szereg wątpliwości interpretacyjnych, jakie pojawiały się na tle poprzednio obowiązujących przepisów. Z drugiej strony natomiast – oceniając zakres i treść wprowadzonych unormowań – nie wydaje się, aby przyjęte rozwiązania odpowiadały rzeczywistym potrzebom i oczekiwaniom, jakie mozna było stawiać przed tego rodzaju regulacją. Co więcej, niektóre z przyjętych rozwiązań trudno uznać za właściwe i spójne z przepisami rozporządzenia 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[7]; dalej: RODO).

Zgodnie z art. 1 ustawy o KZP określa ona zasady tworzenia, organizowania i działania u pracodawcy kasy zapomogowo-pożyczkowej (dalej: KZP) oraz jej likwidacji. Zważywszy na tak ujęty zakres przedmiotowy tego aktu, uznać trzeba, że uregulowane w nim zagadnienia z zakresu ochrony danych osobowych powinny być traktowane jako należące do zakresu organizowania i działania u pracodawcy KZP. Treść tychże unormowań jest jednak wycinkowa. Ustawa o KZP zagadnieniom przetwarzania danych osobowych poświęca art. 43, w którym reguluje wybrane kwestie z tego zakresu. Dodatkowo w innych przepisach ustawy przyjęto rozwiązania, w pewnej mierze odnoszące się do zagadnień ochrony danych osobowych, ale i tak nie pozwala to na uznanie, iż mamy do czynienia z regulacją w tym zakresie o charakterze kompleksowym.

W tym stanie rzeczy przedmiotem analiz prowadzonych w niniejszym opracowaniu jest omówienie i próba oceny unormowań z zakresu ochrony danych osobowych zawartych w ustawie o KZP, jak również wskazanie szeregu kwestii, które mogą się pojawić podczas jej stosowania, a których nie uwzględniono.

Podążając śladem kluczowych kwestii dla ochrony danych osobowych w kontekście funkcjonowania KZP, prowadzone rozważania będą dotyczyć aspektu podmiotowego, na co składa się przede wszystkim ustalenie, komu w tym przypadku przysługuje status administratora oraz scharakteryzowanie grupy podmiotów uprawnionych, które na gruncie RODO określane są jako „osoby, których dane dotyczą". W dalszej kolejności przyjrzymy się jakże istotnym chociażby dla właściwego spełnienia obowiązku informacyjnego podstawom przetwarzania danych osobowych przez KZP, jak również wskażemy na inne podmioty, które w tym procesie uczestniczą. Na zakończenie wspomniane zostaną zagadnienia o charakterze dokumentacyjno-organizacyjnym i technicznym, do czego podstawę znajdziemy zarówno w przepisach ustawy o KZP, jak i w RODO.

ADMINISTRATOR DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z DZIAŁANIEM KZP

Na gruncie przepisów o ochronie danych osobowych określenie, komu w konkretnych okolicznościach przysługuje status administratora, jest jedną z bardziej doniosłych kwestii. Ocena w tym przedmiocie rzutuje bowiem na to, w jaki sposób ukształtowany zostanie system ochrony danych

[7] Dz.U. UE. L. z 2016 r. nr 119, s. 1, z późn. zm.

osobowych oraz komu zostanie przypisana odpowiedzialność za wykonywanie obowiązków z zakresu ochrony danych osobowych i konsekwencje jego naruszenia. W przypadku KZP oceny w tym zakresie dokonywać należy, biorąc pod uwagę zarówno przepisy RODO, jak i ustawy o KZP.

Dla prawidłowego uchwycenia tej problematyki konieczne jest poczynienie pewnych wstępnych założeń dotyczących tego, w jaki sposób przepisy RODO kształtują status takiego podmiotu i w jaki sposób jest on wyodrębniany. Tak więc zgodnie z art. 4 pkt 7 RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Wyjaśnienia wymaga, że wśród podmiotów zobowiązanych do stosowania RODO to właśnie administrator jest podmiotem kluczowym i – obrazowo rzecz ujmując – domyślnie zobowiązanym realizować obowiązki wynikające z tego aktu[8]. Jednocześnie jest podmiotem ponoszącym najdalej idącą odpowiedzialność w przypadku naruszenia przepisów z zakresu ochrony danych osobowych[9]. W konsekwencji zatem to właśnie administrator jest odpowiedzialny za realizację przepisów określających procedury postępowania z danymi osobowymi, nawet jeśli w przepisach prawa nie jest wskazany wprost jako zobowiązany. Wszystkie przepisy określające warunki zgodnego z prawem przetwarzania uznawać należy zatem za z zasady skierowane do administratora, także wówczas, gdy nie wyrażono tego wprost. Tak jest w przypadku tzw. przesłanek dopuszczalności przetwarzania danych osobowych według RODO, a więc art. 6 określającego wymogi zgodnego z prawem przetwarzania danych oraz art. 9 ust. 2, w którym wskazano na zgodne z prawem postawy przetwarzania szczególnych kategorii danych osobowych[10].

W art. 4 pkt 7 RODO określone zostały kategorie podmiotów, którym potencjalnie może przysługiwać status administratora w konkretnych okolicznościach, o ile w danym przypadku o tym, kto jest administratorem, nie decyduje przepis prawa. Owo skategoryzowanie podmiotowe nie jest jednak wystarczające, ponieważ warunkiem przesądzającym o zaliczeniu danego podmiotu do kategorii administratorów danych osobowych jest to, czy w konkretnych okolicznościach decyduje on o celach i sposobach przetwarzania danych osobowych. Elementy te łącznie pozwalają mówić o sprawowaniu władztwa w procesie przewarzania, z którym RODO wiąże wiele obowiązków[11]. Administratorem nie jest zatem każdy podmiot dysponujący danymi osobowymi, a tylko ten, który decyduje o celach i sposobach ich przetwarzania[12].

W wytycznych Europejskiej Rady Ochrony Danych (EROD) 07/2020 przyjętych 7.07.2021 r. dotyczących koncepcji administratora i podmiotu przetwarzającego w RODO[13] pojęcie admini-

[8] Zob. M. Sakowska-Baryła, *Komentarz do art. 4 pkt 7*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 105.

[9] K. Wygoda, *Administrator danych w administracji publicznej*, [w:] *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, red. M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, Wrocław 2018, s. 16.

[10] Opinia 1/2010 Grupy Roboczej Art. 29 przyjęta w dniu 16 lutego 2010 r. w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169).

[11] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 53.

[12] Wyrok NSA z 30 stycznia 2002 r., II SA 1098/01, Lex.

[13] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf [dostęp: 24.9.2021]; dalej: wytyczne 07/2020.

stratora (podobnie jak i pojęcie podmiotu przetwarzającego) określone jest jako „pojęcie funkcjonalne", które ma na celu przypisanie odpowiedzialności zgodnie z rzeczywistymi rolami stron, co oznacza, że status prawny „administratora" musi, co do zasady, być określony przez jego rzeczywistą działalność w określonej sytuacji, a nie opierać się na formalnym lub umownym nadaniu ról podmiotom uczestniczącym w procesach przetwarzania danych osobowych. Potwierdza to trafność interpretacji, wedle której określenie statusu podmiotowego następuje na podstawie analizy stanu faktycznego. Z rzeczonym stanem faktycznym związane są natomiast określone przepisami prawa obowiązki oraz innego rodzaju konsekwencje prawne[14]. Termin „administrator" jest zatem pojęciem funkcjonalnym w tym rozumieniu, że opiera się na faktach w miejsce formalnej analizy, choć mogą być tu wykorzystywane pewne zasady praktyczne i domniemania służące uproszczeniu procesu jego wyodrębniania[15]. Przywołana argumentacja zawarta w wytycznych 07/2020 jest uzasadniona, zwłaszcza że bazowym założeniem przyświecającym określeniu, komu przysługuje status administratora, jest zapewnienie rozliczalności i skutecznej, kompleksowej ochrony danych osobowych, co z kolei ma sprzyjać jak najbardziej efektywnej i kompleksowej ochronie osób, których dane dotyczą, aby zapewnić pełne działanie unijnego prawa o ochronie danych, aby uniknąć luk i zapobiegać możliwemu obchodzeniu przepisów[16]. Na poparcie tej tezy ERPD przywołuje zresztą dorobek orzecznictwa[17]. Jednocześnie jednak nie można tracić z pola widzenia, że owemu funkcjonalnemu wyodrębnieniu administratora musi towarzyszyć faktyczna i prawna zdolność wykonania wszystkich obowiązków wiążących się z takim zakwalifikowaniem podmiotowym.

W art. 43 ust. 7 ustawy o KZP zostało wyraźnie przesądzone, iż „administratorem danych osobowych jest KZP". Zapis ten bynajmniej nie rozwiązuje wszystkich kwestii wątpliwych, które mogłyby się pojawić w zakresie właściwego określania, kto jest kim w procesie przetwarzania danych osobowych przetwarzanych w związku z działaniem kasy.

RELACJA MIĘDZY KASĄ A PRACODAWCĄ W KONTEKŚCIE PRZYMIOTU ADMINISTRATORA DANYCH

Na stronie internetowej Urzędu Ochrony Danych Osobowych nadal dostępne pozostają wyjaśnienia, jakie sformułowane zostały – jeszcze na bazie poprzednio obowiązującej, choć modelowo zbieżnej regulacji – w odpowiedzi na pytanie *kto jest administratorem w przypadku PKZP działającej przy pracodawcy*[18]. Wskazano, że „przesądzenie, jaki jest status Pracowniczej Kasy Zapomogowo-Pożyczkowej (PKZP) działającej u danego pracodawcy i który z podmiotów (PKZP czy zakład pracy) jest, w świetle przepisów o ochronie danych osobowych, administratorem danych osobowych przetwarzanych w związku z działaniem PKZP,

[14] Zob. M. Sakowska-Baryła, *Administrator i podmiot przetwarzający w wytycznych 07/2020 EROD*, [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, red. G. Sibiga, dodatek MoP 23/2021, s. 85-86.

[15] Zob. wytyczne 07/2020.

[16] Ibidem, s. 9.

[17] Zob. wyrok TSUE z 13 maja 2014 r. w sprawie *Google Spain SL i Google Inc.* przeciwko *Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, C-131/12, Legalis, pkt 34; wyrok TSUE z 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, Legalis, pkt 28; wyrok TSUE z 29 lipca 2019 r. w sprawie *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV*, C-40/17, Legalis, pkt 66.

[18] https://uodo.gov.pl/pl/225/1619 [dostęp: 20.01.2022].

wymaga przede wszystkim dokonania analizy konkretnych przepisów mających zastosowanie w określonej sytuacji". W interpretacji organu zarówno pracodawca, jak i pracownicza kasa zapomogowo-pożyczkowa, w zakresie przetwarzanych przez siebie danych osobowych, samodzielnie ustalają własne cele i sposoby ich przetwarzania, co oznacza, że powinni być traktowani jako oddzielni administratorzy, z tym jednak zastrzeżeniem, że w tym obszarze, w którym pracodawca udziela kasie pomocy przy realizacji jej zadań, podmioty te współdziałają ze sobą, wspólnie ustalając cele i sposoby przetwarzania, co oznacza, że można je uznać za współadministratorów. Tym samym w poprzednim stanie prawnym organ nadzorczy odrzucił koncepcję przetwarzania danych osobowych przez podmioty pozostające w takiej właśnie relacji na zasadzie powierzenia przetwarzania danych osobowych.

Mając na uwadze to, że obecnie obowiązująca ustawa w zasadzie powiela regulacje odnośnie do roli, jaką pracodawca odgrywa podczas funkcjonowania KZP, uzasadnionym jest przybliżenie instytucji współadministrowania w zakresie wynikającym z RODO. Administrowanie danymi osobowymi może przyjąć postać współadministrowania, co wynika bezpośrednio z przytoczonej definicji zawartej w art. 4 pkt 7 RODO. Administratorem może być ten z wymienionych w tym przepisie podmiotów, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Z regulacją tą koresponduje treść art. 26 RODO, który w ust. 1 zd. 1 wskazuje, że jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W wytycznych 07/2020 EROD wyjaśniono, że wspólny udział we współadministrowaniu może przyjmować postać wspólnej decyzji (*common decision*), bądź też zbieżnych decyzji (*coverging decisions*) dwóch lub więcej podmiotów. W tym drugim wariancie chodzi o sytuację, gdy decyzje co najmniej dwóch podmiotów się uzupełniają i są niezbędne, by przetwarzanie mogło mieć miejsce, w taki sposób, że mają rzeczywisty (*tangible*) wpływ na określenie celów i sposobów przetwarzania. Istotnym kryterium zatem jest to, że przetwarzanie nie byłoby możliwe bez udziału obu stron, ponieważ jest nierozłączne (nierozerwalnie) połączone. W tej sytuacji wspólny udział obejmuje z jednej strony określenie celów, a z drugiej strony określenie środków[19].

Należy podkreślić, że w ostatnich latach w drodze ustaleń dokonanych w orzecznictwie TS – w wyrokach: z 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16)[20], z 10 lipca 2018 r. w sprawie *Tietosuojavaltuutettu przeciwko Jehovan todistajat – unskonnollinen yhdyskunta* (C-25/17)[21], z 29 lipca 2019 r. w sprawie *Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV* (C-40/17)[22] – doszło do doprecyzowania sposobu rozumienia konstrukcji współadministrowania w obszarze oceny ról poszczególnych współadministratorów w ramach procesu przetwarzania danych. W efekcie tych ustaleń przyjęto, że cel przetwarzania danych osobowych nie musi być wspólny dla współadministratorów w takim rozumieniu, że każdy z nich może przetwarzać dane osobowe

[19] Zob. wytyczne 07/2020.

[20] Wyrok TS z 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, Lex.

[21] Wyrok TS z 10 lipca 2018 r. w sprawie *Tietosuojavaltuutettu przeciwko Jehovan todistajat – unskonnollinen yhdyskunta*, C-25/17, Lex.

[22] Wyrok TS z 29 lipca 2019 r. w sprawie *Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV*, C-40/17, Lex.

dla własnego celu, które to cele w sumie składają się na cel przetwarzania danych w ramach procesu przetwarzania objętego współadministrowaniem. Przy takim podejściu nie ma więc racji bytu wymóg wspólnoty celów przetwarzania. Każdy ze współadministratorów może bowiem podejmować decyzje dotyczące własnego celu przetwarzania, a dopiero suma tych celów pozwala wskazać cel, w którym odbywa się wspólne przetwarzanie[23]. Tym niemniej dla zakwalifikowania danej relacji pomiędzy różnymi podmiotami jako współadministrowanie oraz przyznania poszczególnym tym podmiotom statusu „współadministratora" nie wystarcza, by pozostawały one w jakiejkolwiek relacji związanej z przetwarzaniem danych osobowych. Ich relacja bowiem nacechowana musi być współdziałaniem przy ustalaniu celów i sposobów przetwarzania także wówczas, gdy współdziałanie to w jakiejś mierze odbywa się z zachowaniem samodzielności administratorów pozostających w tej relacji. Wydaje się, że tak właśnie będzie w przypadku KZP i pracodawcy, o ile podzielimy zapatrywanie Prezesa UODO, że w pewnym zakresie funkcjonowania kasy i współpracy pomiędzy nią a pracodawcą mamy do czynienia ze współadministrowaniem.

W tym kontekście rozważań podnieść należy, że w praktyce stosunek współadministrowania zwykle znajduje potwierdzenie w postanowieniach umownych – umowie lub porozumieniu łączącym współadministratorów. W tego rodzaju dokumencie strony określają zakres swoich uprawnień i obowiązków, na co zresztą wskazuje treść art. 26 ust. 1 zd. 2 i 3 oraz i 2 RODO. Z przepisów tych wynika bowiem, że w drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą (26 ust. 1 zd. 2 i 3 RODO). Jednocześnie, jak wynika z art. 26 ust. 2 RODO, uzgodnienia, o których tu mowa, mają należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą, a zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą. Należy również podnieść, że w myśl art. 26 ust. 3 RODO, niezależnie od uzgodnień, o których mowa w art. 26 ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów. W uzupełnieniu tych ustaleń konieczne jest, by wskazać, że stosunek współadministrowania może mieć swoje źródło w przepisach prawa, które mogą wprost wskazywać na określone podmioty jako na współadministratorów w rozumieniu art. 26, jak i określać kryteria ich wyznaczania[24].

[23] Zob. P. Litwiński, *Sprawa Fashion ID a współadministrowanie danymi*, „ABI Expert" 2019, nr 2, s. 52; I. Kwalczuk-Pakuła, M. Chołuj, *Współadministrowanie – nowy paradygmat w prawie ochrony danych osobowych*, [w:] *Prawo nowych technologii dane osobowe i cyberbezpieczeństwo, Internet i media, handel elektroniczny, prawo IT, technologie*, X. Konarski (red.), „Monitor Prawniczy" 2019, nr 21 – dodatek, s. 14 i n.

[24] Ze współadministrowaniem wskazanym wprost w przepisach ustawy mamy do czynienia np. w art. 14ha ust. 1 ustawy o ochronie przeciwpożarowej; art. 24 c ust. 1 ustawy o Państwowym Ratownictwie Medycznym; art. 8a ust. 2 ustawy o zasadach zarządzania mieniem państwowym; art. 10 ust. 5 ustawy o systemie powiadamiania ratunkowego.

Pamiętać należy, że współadministrowanie, podobnie jak administrowanie, to stan faktyczny, który ma charakter obiektywny, co oznacza, że nie jest uzależniony od tego, w jaki sposób rola poszczególnych podmiotów w przetwarzaniu danych osobowych zostaje nazwana w umowie dotyczącej ich współdziałania. Nie można więc mówić o współadministrowaniu w rozumieniu RODO w sytuacji, gdy z okoliczności faktycznych wynika, że relacja konkretnych podmiotów to w istocie układ podmiotów będących osobnymi administratorami niepozostającymi w stosunku współadministrowania, bądź też w danym przypadku mamy do czynienia z administratorem i podmiotem przetwarzającym[25].

Ustawa o KZP nie określa relacji, w jakiej z punktu widzenia ochrony danych osobowych pozostają chociażby KZP i pracodawca. Wydaje się, iż w praktyce uprawnione będzie dochodzenie do ustaleń podobnych do tych, jakie w przywołanym wyżej stanowisku wyraził organ nadzorczy. Rzecz jasna pod uwagę należy brać w tym przypadku relacje zachodzące pomiędzy KZP a pracodawcą. Ustawa o KZP w art. 43 ust. 7 stanowi, że administratorem danych osobowych jest KZP. Natomiast w art. 43 ust. 8 wskazuje, że pracodawca, u którego funkcjonuje KZP, przetwarza dane osobowe, o których mowa w ust. 2, w celu świadczenia KZP pomocy, o której mowa w art. 6 ust. 1 pkt 4-8.

Ustawa nie określa jednak tak określonej relacji wprost jako „współadministrowanie". Daje tylko wyraźną podstawę prawną do działania przez pracodawcę w zakresie współpracy z KZP. Uzupełniająco trzeba tu wskazać, że zgodnie z art. 6 ust. 1 ustawy o KZP pracodawca świadczy KZP pomoc w zakresie:

1) udostępniania pomieszczeń biurowych;

2) udostępniania odpowiednio zabezpieczonego miejsca na przechowywanie gotówki;

3) transportu gotówki do banku i z banku, jeśli pracodawca prowadzi obrót gotówkowy;

4) udzielania informacji umożliwiających dokonanie weryfikacji, czy określona osoba spełnia warunki, o których mowa w art. 7 ust. 1 oraz art. 35 ust. 4 pkt 1-3;

5) prowadzenia rachunkowości, obsługi kasowej i prawnej;

6) dokonywania na rzecz KZP potrąceń wpisowego, miesięcznych wkładów członkowskich i rat pożyczek na listach płac, listach wypłat i zasiłków, a w przypadku braku możliwości dokonania takiego potrącenia – informuje o tym zarząd;

7) niezwłocznego odprowadzania wpłat wpisowego, miesięcznych wkładów członkowskich i rat pożyczek na rachunek płatniczy KZP;

8) przekazywania przez zarząd członkom KZP informacji o stanie ich wkładów członkowskich i zadłużenia.

W myśl art. 6 ust. 2 ustawy o KZP szczegółowe warunki świadczenia pomocy, o której mowa w art. 6 ust. 1, określa umowa zawarta między pracodawcą a KZP, która – jak wynika z art. 6 ust. 2 – może określać zasady wykonywania czynności podejmowanych u pracodawcy przez członków KZP w związku z realizacją ich obowiązków w zarządzie i komisji rewizyjnej. Można więc uznać, że w tej właśnie umowie mogą zostać zawarte postanowienia odpowiadające art. 26 RODO, a więc kształtujące treść stosunku współadministrowania.

W naszej ocenie, z uwagi na to, iż zakres świadczonej przez pracodawcę pomocy na rzecz KZP został określony w art. 6 ustawy o KZP, możliwa jest również interpretacja, iż

[25] M. Sakowska-Baryła, Komentarz do art. 26, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 300.

pracodawca jest odrębnym administratorem danych osobowych przetwarzanych w ramach tej pomocy. Bowiem mimo że ustawa wymaga zawarcia umowy, w której strony, tj. pracodawca i kasa, określają szczegółowe warunki świadczenia pomocy przez pracodawcę, należy stwierdzić, iż pomoc ta jest obowiązkiem prawnym pracodawcy, od wykonania którego uchylić się nie może. Z art. 6 ustawy wynika bowiem, że pracodawca „świadczy" pomoc na rzecz KZP, a nie że „może ją świadczyć". Taki kierunek wykładni jest również uzasadniony wykładnią historyczną. W zarządzeniu z 1983 r. § 6 wyraźnie stanowił, iż kasa w swej działalności korzysta z nieodpłatnej pomocy zakładu pracy, w którym jest utworzona. Zakres tych „obowiązków" był już wówczas zbliżony do obecnego. Podobną do obecnej treść odnajdziemy także w rozporządzeniu z 1992 r.

Do konstrukcji współadministrowania danymi będzie można jednak powrócić wówczas, gdy będziemy mieć do czynienia z działaniem międzyzakładowej KZP, obejmującej zakresem swojego działania co najmniej dwóch pracodawców. Zgodnie z art. 8 ust. 4 pracodawcy, których zakresem swego działania obejmuje międzyzakładowa KZP, zawierają umowę określającą szczegółowe warunki świadczonej KZP pomocy. Podobnie jak to zostało wcześniej wskazane, w umowie tej mogą zostać zawarte postanowienia odpowiadające art. 26 RODO, a więc kształtujące treść stosunku współadministrowania danymi osobowymi przez pracodawców i KZP.

PODMIOT SPRAWUJĄCY NADZÓR JAKO ADMINISTRATOR DANYCH OSOBOWYCH

Jak się wydaje, z pola widzenia ustawodawcy w zakresie przetwarzania danych osobowych zupełnie zniknął podmiot sprawujący nadzór nad KZP. Niezależnie od tego, czy podmiotem tym będzie zakładowa organizacja związkowa, wspólna reprezentacja związkowa organizacji szczebla podstawowego, rada pracowników czy też reprezentacja osób wykonujących pracę zarobkową wyłoniona w trybie przyjętym u pracodawcy, uprawnienia kontrolne są tożsame. Należy zwrócić w szczególności uwagę na jedną kwestię, a mianowicie na obowiązek przekazywania przez KZP podmiotowi sprawującemu kontrolę protokołów z posiedzeń organów KSP oraz protokołów z kontroli działalności KSP sporządzonych przez komisję rewizyjną.

Jeżeli przyjrzymy się uważnie zakresowi działania organów KZP, trudno nie dostrzec, iż kasa będzie w ten sposób przekazywała podmiotowi sprawującemu kontrolę dane osobowe zarówno swoich członków, jak również poręczycieli. Przykładowo z art. 23 ustawy o KZP wynika, iż protokół sporządza się chociażby z każdego posiedzenia zarządu KSP. Posiedzenia odbywają się w miarę potrzeby, nie rzadziej jednak niż raz w miesiącu. Do kompetencji zarządu KZP w szczególności należy przyjmowanie członków i skreślanie ich z listy (odbywa się to w formie uchwał), przyznawanie pożyczek i ustalanie okresu ich spłaty, podejmowanie decyzji w prawie zwolnienia lub odroczenia spłaty pożyczek, udzielanie zapomóg. Nie sposób nie zauważyć, iż wszystkie te kwestie będą znajdowały odzwierciedlenie w treści protokołu z posiedzenia zarządu, który każdorazowo ma być przekazywany podmiotowi sprawującemu kontrolę, który w naszej ocenie od chwili otrzymania takiego protokołu stanie się administratorem danych. Kwestią wymagającą odrębnej refleksji jest to, czy takie protokoły mogłyby zostać zanonimizowane przed przekazaniem. Wydaje się,

iż jest to uzasadnione z uwagi na zasadę minimalizacji danych, zwłaszcza że jest jeszcze komisja rewizyjna, która jako organ kontrolujący działalność finansową zarządu ma w zakresie swoich kompetencji ochronę mienia kasy i czuwanie nad prawidłowym dokumentowaniem wszystkich wpłat i wypłat (art. 28 ustawy o KZP).

Regulacje odnośnie do formy i sposobu przekazywania protokołów zawierających dane osobowe mogłyby się znaleźć w statucie KZP. Zgodnie z art. 15 ust. 1 pkt 15 w statucie określa się m.in. zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia. Poruszony problem jest jednak bez wątpienia jedną z tych kwestii, które wymagają uwagi i odrębnej analizy.

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Administrator nie musi samodzielnie wykonywać operacji przetwarzania danych osobowych, a nawet fizycznie ich posiadać. Czynności przetwarzania mogą być przez niego zlecone na zewnątrz podmiotowi, który na gruncie RODO nazywany jest „podmiotem przetwarzającym", a w praktyce określany także jako „procesor". Jak stanowi art. 4 pkt 8 RODO, „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Powierzenie przetwarzania danych osobowych jest sposobem dokonywania operacji na danych osobowych powszechnym w biznesie i w sektorze publicznym, gdzie podmiot przetwarzający wykonuje czynności przetwarzania danych dla administratora, realizując jego cele i potrzeby – w jego imieniu i na jego rzecz. Uzasadnione jest brać je pod uwagę także w przypadku działania KZP i pracodawców, ponieważ także te podmioty mogą korzystać z zewnętrznych dostawców usług. Treść art. 4 pkt 8 RODO wskazuje, że status podmiotu przetwarzającego może przysługiwać tym samym podmiotom, które w myśl art. 4 pkt 7 RODO mogą być administratorem, ale że różnica między nimi odnosi się do sfery władztwa w procesie przetwarzania danych osobowych, a więc do decydowania o celach i sposobach ich przetwarzania. Sfera ta należy bowiem wyłącznie do administratora. Oznacza to, że podmiot przetwarzający nie może, przetwarzając dane osobowe w imieniu administratora, wychodzić poza zakres powierzonych czynności, a więc realizować własnych celów przetwarzania[26]. Pamiętać jednak należy, że ten sam podmiot może równocześnie występować w podwójnej roli i obok przetwarzania dla innych pozostawać jednocześnie administratorem względem danych osobowych oraz czynności przetwarzania wykonywanych we własnych celach i we własnym imieniu. To powoduje, że konieczne jest wyraźne wytyczanie granic pomiędzy przetwarzaniem realizowanym w charakterze procesora a przetwarzaniem we własnych celach i na własną rzecz[27].

Przedmiotem powierzenia może być dokonywanie każdej operacji przetwarzania, o której mowa w art. 4 pkt 2 RODO, bądź pewnego zespołu takich operacji. Przypomnieć więc należy, że przetwarzanie – zgodnie z art. 4 pkt 2 RODO – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie,

[26] Zob. wyrok WSA w Warszawie z 27 października 2020 r., II SA/Wa 310/20.
[27] M. Sakowska-Baryła, *Komentarz do art. 4 pkt 8,* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 108-109.

porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[28]. Powierzenie przetwarzania wymaga udokumentowania w postaci umowy lub innego instrumentu prawnego, o czym stanowi art. 28 ust. 3 RODO.

Tak więc jeżeli przedmiotem świadczenia na rzecz „zlecającego" są takie czynności, jak w przytoczonej wyżej definicji, należy przyjmować, że mamy do czynienia z relacją powierzenia, w której podmiot wykonujący tego rodzaju czynności dla administratora jest podmiotem przetwarzającym. Brak pisemnej umowy lub innego aktu prawnego (innego instrumentu prawnego) – jak wymaga art. 28 ust. 9 RODO[29], nie oznacza, że w danym przypadku powierzenie przetwarzania nie wystąpiło. Brak takiej umowy lub innego aktu kwalifikować należy jako naruszenie przepisów RODO, a klasyfikowanie podmiotów odpowiednio jako „administrator" i „podmiot przetwarzający" ma charakter obiektywny i następuje w związku z konkretnymi okolicznościami, podejmowanymi decyzjami gospodarczymi, oceną, kto podejmuje decyzje co do celu przetwarzania oraz sposobów, jakimi się ono odbywa[30]. Powierzenie przetwarzanie to stan faktyczny, którego nie zmienia umowne określenie statusu podmiotów pozostających w tej relacji[31].

Próba umownego – nominalnego – oznaczenia ról, analogicznie, jak to ma miejsce w przypadku przekroczenia przez procesora zakresu powierzenia, może prowadzić do konsekwencji opisanych w art. 28 ust. 10 RODO, zgodnie z którym bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania[32]. Przypomnieć tu należy, że przywołane przepisy art. 82, 83 i 84 dotyczą odpowiedzialności za szkodę majątkową lub niemajątkową oraz nakładania administracyjnych kar pieniężnych.

Niezależnie od wcześniej opisanych relacji podmiotowych pomiędzy administratorami danych osobowych przetwarzanych w związku z działaniem KZP nie można wykluczyć, iż pomiędzy tymi podmiotami może również dojść do powierzenia przetwarzania danych osobowych. Tytułem przykładu można wskazać powierzenie przez KZP pracodawcy przechowywania w archiwum zakładowym dokumentów dot. byłego członka kasy. Jak wynika z treści art. 43 ust. 5 pkt 1, KZP przetwarza dane osobowe do upływu 10 lat od dnia ustania członkostwa. Oznacza to, że dane wskazane w art. 43 powinny być przez ten czas przechowywane w sposób gwarantujący ich integralność i poufność. Nietrudno się domyślić, iż kasa może być zainteresowana przekazaniem danych na przechowanie pracodawcy. Czynność ta przekracza zakres pomocy, do udzielania której pracodawca jest ustawowo zobligowany, a zatem jak się wydaje, do rozważenia będzie zawarcie w takiej sytuacji umowy powierzenia przetwarzania.

---

[28] Zob. M. Sakowska-Baryła, *Komentarz do art. 4 pkt 8*…, s. 106.

[29] Zgodnie z art. 28 ust. 9 RODO umowa lub inny akt prawny, o których mowa w ust. 3 i 4, mają formę pisemną, w tym formę elektroniczną.

[30] Opinia 1/2010 Grupy Roboczej Art. 29 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169).

[31] G. Sibiga, *Powierzenie przetwarzania danych osobowych w obrocie gospodarczym*, [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, Warszawa 2013, s. 105-106.

[32] Zob. wyrok WSA w Warszawie z 27 października 2020 r., II SA/Wa 310/20.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH NA PODSTAWIE USTAWY O KZP

Ustawa o KZP w art. 43 ust. 1 stanowi, że przetwarzanie przez KZP danych osobowych w celu realizacji zadań ustawowych związanych z członkostwem w KZP, w tym gromadzenie wkładów członkowskich oraz udzielanie pomocy materialnej w formie pożyczek lub zapomóg, a także dochodzenie związanych z nimi praw lub roszczeń, następuje na podstawie zgody udzielonej w formie oświadczenia członka KZP, osoby uprawnionej lub poręczyciela. Należy zauważyć, że zgoda powinna być zakwalifikowana jako nieadekwatna podstawa przetwarzania danych osobowych, a nawet prawnie i prakseologicznie nieakceptowalna.

Wyjaśnić w tym miejscu należy, że na gruncie RODO ustaleń co do dopuszczalności przetwarzania danych osobowych dokonywać należy w oparciu o treść art. 5 tego aktu, który nosi tytuł „Zasady przetwarzania danych osobowych", oraz odpowiednio – w zależności od tego, czy przetwarzanie dotyczy tzw. danych zwykłych czy też szczególnych kategorii danych – biorąc pod uwagę tzw. przesłanki dopuszczalności przetwarzania danych osobowych określone w art. 6 RODO zatytułowanym „Zgodność przetwarzania z prawem" oraz art. 9 RODO zatytułowanym „Przetwarzanie szczególnych kategorii danych osobowych". Tak więc ocena, czy w konkretnym przypadku dopuszczalne przetwarzanie danych osobowych polega na ustaleniu, czy znajduje ono usprawiedliwienie w przypadku danych zwykłych w treści art. 6 ust. 1 RODO, w przypadku danych wrażliwych w treści art. 9 ust. 2 RODO przy jednoczesnym uwzględnieniu zasad określonych w art. 5, wyznaczających pewne standardy tego przetwarzania i zbiorczo nazywane bywają „zasadami rozliczalności przetwarzania". Dla zgodnego z prawem przetwarzania danych osobowych nie w każdym przypadku wymagana jest zgoda na przetwarzanie danych osobowych, ponieważ zarówno art. 6, jak i art. 9 RODO określają szereg innych przesłanek dopuszczalności przetwarzania danych osobowych, które w konkretnych przypadkach uzasadniają to przetwarzanie. Tak właśnie być powinno w przypadku podstaw przetwarzania danych osobowych przez KZP. Podstawą tą – wbrew niefortunnej decyzji ustawodawcy – nie powinna być zgoda.

Należy w tym miejscu wskazać na treść art. 6 ust. 1 RODO, który stanowi, że przetwarzanie jest zgodne z prawem wyłącznie w wymienionych przypadkach i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) 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;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) 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,

Przy czym – jak wprost wskazane zostało w art. 6 ust. 1 *in fine* – akapit pierwszy lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

W uzupełnieniu podstaw prawnych przetwarzania danych osobowych wyjaśnić również trzeba, że zgodnie z art. 9 ust. 1 RODO zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Tak określone kategorie danych osobowych RODO określa mianem szczególnych kategorii danych (w motywie 10 RODO mowa też o danych wrażliwych). Praktyka natomiast posługuje się przywołaną już wyżej kategoryzacją danych osobowych uzyskiwaną dzięki podziałowi na dane zwykłe i szczególne kategorie danych, gdzie kryterium rozróżnienia pozostaje zaliczenie informacji odpowiednio do tych, o których mowa w art. 9 ust. 1 RODO, bądź do takich, które nie są w tym przepisie wymienione, co powoduje, że mają nie szczególny, ale zwykły charakter, a zatem nazywa się je danymi zwykłymi. W tym stanie rzeczy pamiętać należy, że podstawy dopuszczalności przetwarzania danych osobowych szczególnych kategorii określa art. 9 ust. 2 RODO, zgodnie z którym ogólny zakaz przetwarzania takich danych wyrażony w ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

b) przetwarzanie jest niezbędne do wypełnienia 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 Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) 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;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Dla uprawnionego przetwarzania wystarczające jest spełnienie jednej przesłanki dopuszczalności przetwarzania danych osobowych z art. 6 lub 9 RODO, choć w praktyce bywa i tak, że przetwarzanie dla jednego celu odbywa się na podstawie więcej niż jednej przesłanki[33].

Prowadzone tu rozważania wymagają jednocześnie sięgnięcia do osobno zdefiniowanej kategorii zgody na przetwarzanie danych osobowych. Zgodnie z art. 4 pkt 11 RODO „zgoda" osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Dodatkowo kwestia zgody na przetwarzanie danych osobowych uregulowana została a art. 7 RODO zatytułowanym „Warunki wyrażenia zgody" Przepis ten w ust. 1 wskazuje, że jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Z art. 7 ust. 2 wynika, że jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, przy czym część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego

[33] Na przykład przetwarzanie danych osobowych związanych z zatrudnieniem lub zawarciem i wykonaniem umowy.

rozporządzenia, nie jest wiążąca. W art. 7 ust. 3 znajduje się zastrzeżenie, że osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę, z tym że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem, a osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Wreszcie w art. 7 ust. 4 klaruje się, że oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Biorąc pod uwagę tak określone w RODO uwarunkowania prawne dotyczące wyrażania zgody na przetwarzanie danych osobowych, nie sposób stwierdzić, że przywołany wyżej przepis ustawy o KZP jest spójny z tą regulacją.

Zgoda, o której mowa w art. art. 43 ust. 1 tej ustawy, nie jest wyrażana w warunkach swobody, co więcej – nie sposób w jej przypadku stwierdzić, że realne jest wynikające z art. 7 ust. 3 RODO jej wycofanie w dowolnym momencie. Oczywiste wydaje się tu pytanie o skutki takiego cofnięcia oraz wątpliwość co do tego, jak kontynuować członkostwo w KZP po cofnięciu zgody na przetwarzanie danych osobowych. Należy co więcej zwrócić uwagę, że w myśl art. 15 pkt 16 ustawy o KZP wzór oświadczenia woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, oraz wskazanie administratora danych osobowych ma określać statut KZP. W naszej ocenie poprawną podstawą przetwarzania danych osobowych członka KZP powinien być przepis prawa. Z chwilą wypełnienia deklaracji członkowskiej podmiot danych przystępuje do pewnej wspólnoty, chcąc korzystać z uprawnień członka kasy uregulowanych ustawowo, jak również poddając się konsekwencjom ustawowym napuszenia swoich obowiązków względem kasy. Zakres jego danych osobowych przetwarzanych w ramach stosunku członkostwa również wydaje się być szerszy od katalogu z art. 43.

ZAKRES DANYCH OSOBOWYCH PRZETWARZANYCH PRZEZ KZP

Zgodnie z art. 4 pkt 1 RODO „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Biorąc pod uwagę tę definicję, każdy administrator, w tym oczywiście KZP, jest zobowiązany sprawować pieczę nad tym, jakie dane osobowe przetwarza i jakich kategorii podmiotów one dotyczą. Zobowiązany jest przy tym dokonać wnikliwej inwentaryzacji tak określonych zasobów informacyjnych, ponieważ w odniesieniu do każdej z kategorii danych osobowych musi dokonać ustaleń co do podstaw przetwarzania (art. 6 i art. 9 RODO) oraz uprawnionego zakresu tego przetwarzania. Ten ostatni obowiązek wyprowadzać należy przede wszystkim z art. 5 RODO, który określa zasady dotyczące przetwarzania danych osobowych, a więc tzw. zasady rozliczalności. W ten sposób RODO kształtuje ogólne wymogi

dotyczące przetwarzania – mające charakter nadrzędny i na swój sposób wyłączone „przed nawias[34]. Zgodnie z art. 5 ust. 1 RODO dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne, do celów, w których są przetwarzane („minimalizacja danych");

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Dodatkowo, jak wynika z art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Tak określone zasady przetwarzania danych osobowych odnoszą się do działalności KZP, która powinna ustalić, jakimi kategoriami danych osobowych dysponuje, kogo te dane dotyczą, na jakiej podstawie prawnej są przetwarzane, w jaki sposób są zabezpieczone, w jaki sposób w związku z ich przetwarzaniem realizuje się prawa osób, których dane dotyczą, o których mowa w rozdziale III RODO itp. Gdy zestawia się tak określone obowiązki z regulacją zawartą w ustawie o KZP, ewidentnie widać, że unormowania te mają charakter mocno szczątkowy i wybiórczy, ponieważ dotyczą tylko pewnych wyodrębnionych osób, których dane dotyczą, oraz pewnych kategorii danych osobowych z pominięciem innych, które jednak muszą pozostawać punktem uwagi osób podejmujących działania na rzecz KZP.

Jak stanowi art. 43 ust. 2 analizowanej ustawy, KZP przetwarza dane osobowe:

1) członka KZP obejmujące:

a) imię (imiona) i nazwisko,

b) numer PESEL, a w przypadku braku numeru PESEL – nazwę i numer dokumentu potwierdzającego tożsamość oraz nazwę państwa, które go wydało,

[34] Zob. M. Krzysztofek, *Komentarz do art. 5, uwaga 1*, [w:] *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.

c) adres do korespondencji oraz numer telefonu lub adres poczty elektronicznej,
d) stan cywilny oraz ustrój majątkowy,
e) stan zdrowia,
f) otrzymywane wynagrodzenie lub zasiłek;
2) osoby uprawnionej obejmujące dane, o których mowa w pkt 1 lit. a-c;
3) poręczyciela, obejmujące dane, o których mowa w pkt 1 lit. a-d.

Nie wydaje się jednak, aby tak określony katalog danych miał charakter zupełny. Z lektury ustawy o KZP wynika bowiem, że kasa przetwarzać będzie także chociażby takie dane, jak: informacje o dacie powstania i ustania członkostwa w KZP, o wpisowym i wkładzie członkowskim, informacje o spłatach pożyczek i zadłużeniu, informacje o numerze rachunku bankowego członka, informacje o funkcjach pełnionych w organach KZP, informacje o miejscu zatrudnienia, co szczególnie istotne w przypadku kas międzyzakładowych, również o tym, gdzie dana osoba jest zatrudniona, informacje o udziale w zebraniach itp. Dane te pozostają jednak poza wyliczeniem zawartym w art. 43 ust. 2 ustawy.

W myśl art. 43 ust. 3 ustawy KZP może żądać udokumentowania danych osobowych w zakresie niezbędnym do ich potwierdzenia, przy czym potwierdzenie może odbywać się w szczególności na podstawie oświadczenia lub zaświadczenia. Istotne też, że aktualizowanie swoich danych osobowych stanowi obowiązek członka KZP, wynikający z art. 12 ust. 1 pkt 5 ustawy.

Dane osobowe, o których mowa w art. 43 ust. 2, mogą być przetwarzane w postaci papierowej lub elektronicznej, zaś sposób przetwarzania danych oraz ich zabezpieczania reguluje statut KZP (art. 43 ust. 9). To przepis skorelowany z wymogami co do treści statutu KZP, ponieważ zgodnie z art. 15 ust. 1 pkt 15 stanowi, że ma on określać zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia.

WYDAWANIE UPOWAŻNIEŃ I TAJEMNICA DANYCH OSOBOWYCH

Jak wynika z art. 43 ust. 4 ustawy o KZP, do przetwarzania danych osobowych, o których mowa w art. 43 ust. 2, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez zarząd. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy oraz ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem.

Z art. 43 ust. 4 nie wynika, czyim obowiązkiem jest wydanie takich upoważnień. Z literalnego brzmienia przepisu należałoby wnioskować, iż jest to wyłączny obowiązek kasy, gdyż mają być wydane przez jej zarząd. Wątpliwość pojawia się jednak już w przypadku, gdy w ramach pomocy ze strony pracodawcy do przetwarzania danych osobowych będą dopuszczone osoby spoza władz kasy, takie chociażby jak pracownicy działu kadr, płac czy działu prawnego. Pomoc na rzecz kasy polega bowiem w szczególności na prowadzeniu rachunkowości, obsługi kasowej i prawnej, dokonywaniu na rzecz KZP potrąceń wpisowego, miesięcznych wkładów członkowskich i rat pożyczek na listach płac, listach wypłat i zasiłków.

Upoważnienia do przewarzania danych osobowych należy potraktować jako jedno z rozwiązań o charakterze techniczno-organizacyjnym służącym bezpieczeństwu tych danych, które może zostać uregulowane w umowie o współadministrowaniu danymi osobo-

wymi, jeżeli relacja między pracodawcą a kasą w taki sposób zostałaby zakwalifikowana. Wydaje się, że gdyby pracodawca miał być samodzielnym administratorem danych, upoważnienia powinny wychodzić od niego.

Warto w tym miejscu zwrócić uwagę na treść art. 24 RODO, który w ust. 1 wskazuje, że uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać, przy czym środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Ponadto – jak wynika z art. 24 ust. 2 RODO – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Obowiązek wprowadzenia takich zabezpieczeń obciąża także KZP jako administratora. Wydaje się, że adekwatne w tym kontekście jest wdrożenie odpowiednich zabezpieczeń oraz polityk ochrony danych. Pomocna może tu okazać się wszelkiego rodzaju dokumentacja, która pozwoli KZP zapewnić rozliczalność przetwarzania (art. 5 ust. 2 RODO). Na dokumentację taką składają się zarówno dokumenty, o których w RODO stanowi wprost, jak chociażby: rejestry prowadzone na podstawie art. 30 RODO, polityki ochrony danych osobowych, o których mowa w art. 24 ust. 2 RODO, dokumentacja dotycząca naruszeń ochrony danych osobowych wymagana przez art. 33 ust. 5 RODO, umowy powierzenia lub inne akty prawne (inne instrumenty prawne), dla których art. 28 ust. 9 RODO wymaga formy pisemnej (w tym elektronicznej), ocena skutków dla ochrony danych osobowych sporządzona zgodnie z art. 35 ust. 7 RODO, jak również wszelkiego rodzaju inna dokumentacja. Takimi dokumentami są także upoważnienia, o których mowa w ustawie o KZP.

Ocena zagrożeń musi być dokonywana w kontekście ryzyka naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze, w ślad za treścią motywu 75 wiązać je należy z przetwarzaniem mogącym prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa. Motyw ten wskazuje również, że jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Analiza ryzyka naruszeń praw lub wolności osób fizycznych stanowi także konieczny element określonych w art. 25 RODO mechanizmów uwzględniania ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych osobowych (*privacy by default*). W wytycznych 4/2019 EROD wskazuje, że te rozwiązania są komplementarne

i wzajemnie się wzmacniają[35]. Zgodnie z art. 25 ust. 1 RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Na podstawie zaś art. 25 ust. 2 RODO administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Wymogi dotyczące obowiązków w zakresie bezpieczeństwa przetwarzania danych osobowych określone zostały w art. 32 RODO. Przepis ten w ust. 1 stanowi, że uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia 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.

Zgodnie z art. 32 ust. 2 RODO, oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Istotne na gruncie RODO jest także, że administrator oraz podmiot przetwarzający mają podejmować działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego (art. 32 ust. 4 RODO). Wszystko jest spójne z wymogiem wdrożenia odpowiednich środków techniczno-organizacyjnych, o których mowa w art. 24 ust. 2 RODO, a także odpowiedniej

[35] EROD Wytyczne 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z artykułu 25, wersja 2.0, przyjęta 20 października 2020 r., s. 5-6, https://uodo.gov.pl/pl/414/1331 [dostęp: 14.07.2021].

dokumentacji osobowej, w tym stosownych poleceń, upoważnień, oświadczeń o zachowaniu w tajemnicy danych osobowych i sposób ich zabezpieczenia, których zastosowanie wynika zarówno z RODO, jak i ustaw, jak również może być wyrazem zapobiegliwości administratora czy podmiotu przetwarzającego w celu wykazania rozliczalności przewarzania, jak i potrzeby bieżącego monitorowania stanu i efektywności wdrożonych rozwiązań[36]. Zgodnie z art. 32 ust. 3 RODO wywiązywanie się z obowiązków, o których tu mowa, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, jednak – jak wyżej wskazano – obecnie w Polsce administratorzy właściwie nie mają możliwości korzystania z takich rozwiązań, skupiając się na tworzonych przez siebie procedurach i dokumentacji[37].

CZAS PRZECHOWYWANIA DANYCH OSOBOWYCH PRZEZ KZP

Zgodnie z art. 43 ust. 5 ustawy o KZP, że KZP przetwarza dane osobowe, wymienione w ust. 2 tegoż artykułu:

1) w zakresie danych osobowych członka kasy – od dnia złożenia oświadczenia, zawierającego zgodę na przetwarzanie danych, do upływu 10 lat od dnia ustania członkostwa;

2) w zakresie danych osobowych osoby uprawnionej – od dnia złożenia oświadczenia zawierającego zgodę na przetwarzanie danych do upływu 5 lat od dnia wypłaty wkładu członkowskiego;

3) w zakresie danych osobowych poręczyciela – od dnia złożenia oświadczenia, zawierającego zgodę na przetwarzanie danych do upływu 5 lat od dnia spłaty poręczanej pożyczki.

Jak wynika z art. 43 ust. 6 ustawy o KZP, upływ tych terminów obliguje administratora – w tym przypadku kasę – do niezwłocznego zniszczenia dokumentów zawierających dane osobowe w wersji papierowej i trwałego ich usunięcia z nośników elektronicznych. Z jednej strony przepis ten zdaje się formułować dość klarowny obowiązek, z drugiej – poprzez przypisanie w tym przepisie roli „administratora" KZP – zupełnie otwartą pozostawia kwestię okresu retencji tych samych danych przetwarzanych przez inne podmioty. Mamy tu w szczególności na myśli zarówno pracodawcę udzielającego pomocy KZP, jak i podmiot sprawujący kontrolę, który również na podstawie regulacji ustawowych stanie się administratorem całego szeregu danych osobowych zawartych w protokołach.

W naszej ocenie wskazane byłoby, aby kwestie te były uregulowane w statucie poprzez doprecyzowanie zakresu danych przekazywanych podmiotom uczestniczącym w procesie funkcjonowania kasy, jej kontroli oraz w regulacjach umownych pomiędzy tymi podmiotami.

Niezależnie od okresów przetwarzania danych w myśl art. 43 ust. 10 ustawy to zarząd KZP dokonuje przeglądu danych osobowych, o których mowa w art. 43 ust. 2, nie rzadziej niż

[36] Szerzej zob.: P. Tobiczyk, *Polityka ochrony danych osobowych*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, red. M. Jagielski, Warszawa 2019, s. 25; M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia*, [w:] *Dokumentacja ochrony danych osobowych…*, s. 247 i n.; M. Cwener, *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych. Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 97 i n.; M. Jagielski, *Dokumentacja ochrony danych osobowych zgodna z RODO*, [w:] *Dokumentacja ochrony danych osobowych…*, s. 13 i n.; M. Sakowska-Baryła, *Dokumentacja audytów wewnętrznych*, [w:] *Dokumentacja ochrony danych osobowych…*, s. 185 i n.

[37] Szerzej zob.: K. Gałęzowska, *Dokumentowanie zgodności z przepisami RODO*, [w:] *Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, „Monitor Prawniczy" 2020, nr 23 – dodatek, s. 42 i n.

raz w roku kalendarzowym w celu ustalenia niezbędności ich dalszego przechowywania, i to zarząd usuwa dane osobowe, których dalsze przechowywanie jest zbędne do realizacji celu określonego w ust. 1. Problem jednak w tym, że nie w każdym przypadku zarząd będzie miał zapewnione adekwatne rozwiązania organizacyjno-techniczne dla dokonania tych czynności. Poza zakresem działania zarządu KZP są, co oczywiste, dane osobowe przetwarzane przez pracodawcę czy organ kontrolujący. Każdy z tych podmiotów w naszej ocenie powinien dokonywać tych czynności, mając na względzie zasadę ograniczenia przechowywania danych.

OCHRONA DANYCH OSOBOWYCH JAKO MATERIA STATUTOWA KZP

Zgodnie z art. 15 ust. 1 pkt 15 i 16 ustawy statut KZP określa: zasady i sposób przetwarzania danych osobowych oraz ich zabezpieczenia i wzór oświadczenia woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, oraz wskazanie administratora danych osobowych. Obydwa te elementy wydają się mocno dyskusyjne.

Jak to już zostało wcześniej podniesione, kwestia zgody jako podstawy przetwarzania danych osobowych jest merytorycznie nieuzasadniona, co czyni zapis w statucie odnośnie do wzoru oświadczenia woli zbędnym. O ile można by zaakceptować, aby statut regulował pewne zasadnicze kwestie z zakresu ochrony danych osobowych, o tyle z uwagi na sposób jego uchwalenia i znaczną dynamikę, jaka cechuje procesy przetwarzania danych i zmieniające się zagrożenia ich integralności i poufności, do rozważenia powinno być opracowanie polityki ochrony danych, której zapisy mogłyby być na bieżąco uzupełniane czy też modyfikowane.

PODSUMOWANIE

W naszej ocenie wydaje się być w pełni uzasadnione dokonanie powtórnego przeglądu uregulowań ustawy o KZP pod kątem ochrony danych osobowych. Jeżeli ustawodawca już podjął się tego, aby uszczegółowić w ustawie zagadnienia związane z przetwarzaniem danych osobowych, powinien to uczynić poprawnie – tu mamy na myśli w szczególności dobór właściwej podstawy prawnej przetwarzania danych – a także kompleksowo. W przeciwnym razie po raz kolejny cały szereg zagadnień pozostawiony zostanie judykaturze i doktrynie, która, jak wiadomo, nie zawsze „mówi jednym głosem", co ma niekorzystny wpływ na budowanie zaufania obywateli do różnego rodzaju rozwiązań prawnych i instytucjonalnych.

Bibliografia

Literatura

Cwener M., *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych*, *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej (red.), Warszawa 2017.

Gałęzowska K., *Dokumentowanie zgodności z przepisami RODO*, [w:] „Aktualne problemy prawnej ochrony danych osobowych" 2020, red. G. Sibiga, „Monitor Prawniczy" 2020, nr 23 – dodatek.

Jagielski M., *Dokumentacja ochrony danych osobowych zgodna z RODO*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, red. M. Jagielski, Warszawa 2019.

Kwalczuk-Pakuła I., Chołuj M., *Współadministrowanie – nowy paradygmat w prawie ochrony danych osobowych*, „Prawo nowych technologii dane osobowe i cyberbezpieczeństwo, Internet i media, handel elektroniczny, prawo IT, technologie", red. X. Konarski, „Monitor Prawniczy" 2019, nr 21 – dodatek

Litwiński P., *Sprawa Fashion ID a współadministrowanie danymi*, „ABI Expert" 2019, nr 2.

Krzysztofek M., *Komentarz do art. 5 uwaga 1,* [w:] *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.

M.P. nr 19, poz. 110, ze zm.

Otto M, *Przetwarzanie danych osobowych w kontekście zatrudnienia*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, red. M. Jagielski, Warszawa 2019.

Sakowska-Baryła M., *Administrator i podmiot przetwarzający w wytycznych 07/2020 EROD*, [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych*, „Aktualne problemy ochrony danych osobowych" 2021, red. G. Sibiga, dodatek MoP 23/2021.

Sakowska-Baryła M., *Dokumentacja audytów wewnętrznych*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, red. M. Jagielski, Warszawa 2019.

Sakowska-Baryła M., *Komentarz do art. 26*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.

Sakowska-Baryła M., *Komentarz do art. 4 pkt 7*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.

Sakowska-Baryła M., *Komentarz do art. 4 pkt 8*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.

Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.

Sibiga G., *Powierzenie przetwarzania danych osobowych w obrocie gospodarczym*, [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, Warszawa 2013.

Tobiczyk P., *Polityka ochrony danych osobowych*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, red. M. Jagielski, Warszawa 2019.

Wygoda K., *Administrator danych w administracji publicznej*, [w:] *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, red. M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, Wrocław 2018.

Akty normatywne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. Nr 119, s. 1, z późn. zm.).

Ustawa z dnia 11 sierpnia 2021 r. o kasach zapomogowo-pożyczkowych (Dz.U. poz. 1666).

Ustawa z dnia 7 kwietnia 2006 r. o informowaniu pracowników i przeprowadzaniu z nimi konsultacji (Dz.U. poz. 550, z 2008 r., poz. 584 i 778 oraz z 2009 r. poz. 805).

Ustawa z dnia 8 października 1982 r. o związkach zawodowych (Dz.U. nr 32, poz. 16, ze zm.).

Ustawa z dnia 7 kwietnia 2006 r. o informowaniu pracowników i przeprowadzaniu z nimi konsultacji (Dz.U. poz. 550, z 2008 r., poz. 584 i 778 oraz z 2009 r., poz. 805).

Orzecznictwo

Wyrok TS z 10 lipca 2018 r. w sprawie *Tietosuojavaltuutettu przeciwko Jehovan todistajat – unskonnollinen yhdyskunta*, C-25/17, Lex.

Wyrok TS z 29 lipca 2019 r. w sprawie *Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV*, C-40/17, Lex.

Wyrok TS z 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, Lex.

Wyrok TSUE z 13.5.2014 r. w sprawie *Google Spain SL i Google Inc.* przeciwko *Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, C-131/12, Legalis

wyrok TSUE z 29 lipca 2019 r. w sprawie *Fashion ID GmbH & Co.KG* przeciwko *Verbraucherzentrale NRW eV*, C-40/17, Legalis.

Wyrok TSUE z 5 czerwca 2018 r. w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, Legalis.

Uchwała SN(7z) z 22 grudnia 1979 r., III CZP 27/79, OSNC 1980, nr 4, poz. 64.

Wyrok WSA w Warszawie z 27 października 2020 r., II SA/Wa 310/20.

Wyrok NSA z 30 stycznia 2002 r., II SA 1098/01, Lex.

Wyrok WSA w Warszawie z 27 października 2020 r., II SA/Wa 310/20.

Dokumenty EROD i Grupy Roboczej Art. 29

Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf,

https://uodo.gov.pl/pl/225/1619.

Wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z artykułu 25, wersja 2.0, przyjęta 20 października 2020 r., s. 5-6, https://uodo.gov.pl/pl/414/1331.

Opinia 1/2010 Grupy Roboczej Art. 29 przyjęta w dniu 16 lutego 2010 r. w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169), https://archiwum.giodo.gov.pl/pl/1520057/3595.