Studia z zakresu prawa pracy i polityki społecznej 2016
ISSN 1429-9585

Jacek Borowicz
Uniwersytet Wrocławski

WŁAŚCIWOŚCI PRACOWNICZEGO OBOWIĄZKU ZACHOWANIA TAJEMNICY DANYCH OSOBOWYCH

Zgodnie z art. 100 § 2 pkt. 5 ustawy z dnia 26 czerwca 1974 r. *Kodeks pracy* (dalej jako k.p.)[1] pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Obowiązek ten aktualizuje się wtedy, gdy dany pracownik z tytułu wykonywania określonego rodzaju pracy lub miejsca, w którym praca jest wykonywana, będzie miał dostęp do informacji objętych tajemnicą określoną w odrębnych przepisach[2]. Jednym z przypadków tajemnicy reglamentowanej prawnie na mocy odrębnych przepisów jest tajemnica danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek jej zachowania przez osoby upoważnione do przetwarzania danych osobowych wynika z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (dalej jako *ustawa o.d.o.*)[3].

Zakres podmiotowy pracowniczego obowiązku zachowania tajemnicy danych osobowych dane osobowe oraz sposobów ich zabezpieczenia

Zgodnie z art. 39 ust. 2 *ustawy o.d.o.* obowiązek zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia ciąży na osobach, które zostały upoważnione do przetwarzania danych osobowych. Kryterium wyodrębnienia osób objętych powinnością określoną w art. 39 ust. 2 *ustawy o.d.o.* nie jest zatem rodzaj więzi prawnej, w ramach której przetwarzają one dane osobowe czy też sam fakt uzyskania dostępu do tych danych i ich faktyczne przetwarzanie[4]. Kryterium tym nie jest również podstawa nawiązania stosunku pracy, rodzaj pracy umówionej, stanowisko pracy czy zawód wykonywany przez dana osobę fizyczną – nawet, jeśli dla realizacja celów objętych danym rodzajem pracy lub zawodem niezbędne jest przetwarzanie danych osobowych. Znaczenia nie ma także to, czy ujawnienie danych osobowych lub sposobów ich zabezpieczenia

---

[1] Dz.U.2014.1502 j.t. ze zm.

[2] Zob. A.M. Świątkowski, *Kodeks pracy. Komentarz*, Warszawa 2006, s. 438–439.

[3] Dz.U.2016.922 j.t.

[4] Podkreśla się także, że osoba upoważniona do przetwarzania danych nie musi być zatrudniona u administratora danych osobowych, upoważnienie może być udzielone także osobie z zewnątrz – zob. J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 39 ustawy o ochronie danych osobowych*, stan prawny 2015.07.01, na stronach www.lex.online.wolterkluwer.pl, dostęp przez www.prawo.uni.wroc.pl, z dn. 5 lutego 2016 r.

może narazić administratora danych na szkodę. Kluczowe znaczenie ma natomiast fakt nadania konkretnej osobie fizycznej przez tegoż administratora upoważnienia do przetwarzania danych osobowych[5]. Z punktu widzenia sytuacji prawnej administratora danych osobowych nadanie takiego upoważnienia oznacza spełnienie przezeń powinności ciążącej na nim na mocy przepisów *ustawy o.d.o.* Pracodawca zatem, występując w odniesieniu do danych osobowych przetwarzanych u siebie jako administrator danych osobowych w rozumieniu art. 7 pkt. 4 *ustawy o.d.o.*[6], dokonuje każdorazowo oceny, którym osobom fizycznym zatrudnianym przez siebie, jako pracownicy w rozumieniu k.p., niezbędny jest do nich dostęp ze względu na umówiony rodzaj pracy. Formalnym wyrazem uznania przezeń, że przetwarzanie danych osobowych jest niezbędne dla prawidłowego wykonania pracy umówionej będzie nadanie pisemnego upoważnienia, na mocy którego indywidualnie, imiennie oznaczonemu pracownikowi zatrudnionemu na konkretnym stanowisku pracy zostanie udzielony dostęp do danych osobowych określonej kategorii i dla potrzeb określonych form ich przetwarzania[7]. Pracodawca, stosownie do swoich potrzeb, różnicować może zakresy dostępu poszczególnych pracowników do różnych kategorii danych osobowych. Może także wskazywać w upoważnieniu, jakie konkretne sposoby przetwarzania danych leżeć będą w zakresie obowiązków danego pracownika[8].

Upoważnienie powinno być nadane pracownikowi przed rozpoczęciem pracy związanej z przetwarzaniem tych danych. Można przyjąć, że nadanie takiego upoważnienia łączyć się może z procedurą zapoznania się pracownika przed dopuszczeniem do pracy z zakresem informacji objętych tajemnicą określoną w obowiązujących ustawach dla umówionego z pracownikiem rodzaju pracy. Pracodawca powinien następnie uzyskać pisemne potwierdzenie faktu zapoznania się pracownika z zakresem danych osobowych i sposobami ich zabezpieczenia, z jakimi będzie on miał do czynienia na swoim stanowisku pracy (§ 3 rozporządzenia MPiPS z dn. 28.05.1996 r. *w sprawie zakresu prowadzenia przez pracodawcę dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika*[9]). Należy przyjąć, że upoważnienie do przetwarzania danych osobowych może być nadane pracownikowi na cały okres zatrudnienia na danym stanowisku a także okresowo, np. w związku z udziałem pracownika w ograniczonym czasowo zadaniu (projekcie) obejmującym tylko część okresu zatrudnienia u danego

---

[5] W konsekwencji mogą być to zarówno pracownicy w rozumieniu art. 2 k.p. jak i osoby zatrudnione na innych podstawach prawnych, o ile legitymują się one stosownym upoważnieniem pracodawcy i, jako takie, zostały ujęte w ewidencji osób uprawnionych do przetwarzania danych osobowych – zob. J. Borowicz, *Sytuacja prawna pracownika przetwarzającego dane osobowe w ramach wykonywania obowiązków ze stosunku pracy*, [w:] *Z aktualnych problemów prawa pracy i prawa socjalnego*, red. H. Szurgacz, Acta Universitatis Wratislaviensis N0 3082, Prawo CCCVII, Wrocław 2009, s. 11.

[6] Zgodnie z art. 7 pkt. 4 *ustawy o.d.o.* administratorem danych osobowych jest organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych

[7] Zob. J. Borowicz, *Obowiązek prowadzenia przez pracodawcę dokumentacji osobowej i organizacyjnej z zakresu ochrony danych osobowych*, PiZS z 2001 r., nr 3, s. 4

[8] Zgodnie z art. 7 pkt. 2 *ustawy o.d.o.* ilekroć jest w niej mowa o przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

[9] Dz.U.96.62.286 z późn. zm.

pracodawcy. Uznaje się, że upoważnienie nadawane być winno nie tylko pracownikom, których praca umówiona ze swej istoty polega na przetwarzaniu danych osobowych, ale także tym, którzy przetwarzają je ubocznie, incydentalnie a nawet jednorazowo[10].

Pracownicy wykonujący pracę związaną z przetwarzaniem danych osobowych u danego pracodawcy, dysponujący odpowiednim upoważnieniem identyfikowani być winni jako administrujący danymi osobowymi w ramach wykonywania obowiązków ze stosunku pracy. Należy ich odróżniać od pracodawcy – administratora danych osobowych będącego podmiotem, który zarządza zbiorem danych lub danymi decydując o celach i środkach ich przetwarzania oraz ponosząc ogólną odpowiedzialność za przetwarzanie ich zgodnie z obowiązującym prawem[11].

Zakres przedmiotowy powinności określonej w art. 39 ust. 2 *ustawy o.d.o.*

Jak wynika z treści art. 39 ust. 2 *ustawy o.d.o.* zakresem obowiązku poufności w nim wyrażonego objęte są dwa obszary – same dane osobowe przetwarzane przez upoważnionego pracownika oraz sposoby ich zabezpieczenia. Upoważniony pracownik ma zatem obowiązek zachować w tajemnicy wszelkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych (art. 6 ust. 1. *ustawy o.d.o.*), jakie są przetwarzane u danego pracodawcy: 1) w ramach wykonywania jego zadań, jako organu państwowego, organu samorządu terytorialnego lub państwowej albo komunalnej jednostki organizacyjnej albo też podmiotu niepublicznego realizującego zadania publiczne, lub 2) w związku z jego działalnością zarobkową, zawodową lub działalnością służącą realizacji jego celów statutowych[12]. Pracownik zachowuje w tajemnicy dane osobowe przetwarzane u danego pracodawcy w każdej formie, a w szczególności: 1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, 2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych (zob. art. 2 ust. 2 *ustawy o.d.o*).

Można przyjąć, że pracodawca typowo administruje danymi osobowymi w dwóch zasadniczych obszarach. Pierwszym będą dane osobowe przetwarzane na zasadach określonych w art. 22^1 § 1–5 k.p. w związku zatrudnieniem pracowników. Można przyjąć, że upoważnionymi pracownikami administrującymi danymi osobowymi będą w tym przypadku osoby zatrudnione w szeroko rozumianych komórkach kadrowych wyodrębnionych w strukturze danego pracodawcy oraz osoby kierujące innymi pracownikami. Drugi obszar wyznaczany będzie zaś przez przedmiot działalności danego pracodawcy. Upoważnienie do przetwarzania danych osobowych niezbędne będzie zatem dla pracowników zatrudnionych przy realizacji jego zadań i celów publicznych, zarobkowych, zawodowych lub statutowych, jeśli z zadaniami tymi i celami wiąże się, choćby ubocznie lub incydentalnie potrzeba dostępu do tego typu danych.

---

[10] Zob. M. Madej, *O dostępie pracownika do baz danych klientów*, PiZS z 2009 r., nr 6, s. 29.

[11] Na ten temat szerzej zob. J. Borowicz, *Sytuacja prawna pracownika przetwarzającego dane osobowe*…, tamże, s. 11–13 i przytaczana tam literatura i orzecznictwo (w szczególności wyrok NSA w Warszawie z dn.30 stycznia 2002 r., II SA 1098/01, Wokanda 2002/7–8/70; postanowienie SN z dnia 11 grudnia 2000 r., II KKN 438/00, OSNKW 2001/3–4/33**)**. Zob. też M. Madej, *O dostępie pracownika…, tamże*, s. 28.

[12] Zob. art. 3 ust. 1–2 *ustawy o.d.o.* określający jej zakres podmiotowy.

Występujące w treści art. 39 ust. 2 *ustawy o.d.o.* określenie „sposoby zabezpieczenia" danych należy odnosić do organizacyjnych, technicznych, osobowych – a w szczególności informatycznych środków stosowanych u danego pracodawcy w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Pamiętać należy, że w świetle z art. 36 ust. 1–2 *ustawy o.d.o.* pracodawca, jako administrator danych osobowych jest obowiązany w szczególności: 1) zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, 2) prowadzić dokumentację opisującą sposób przetwarzania danych oraz środki ochrony danych. Ponadto, zgodnie z art. 36a *ustawy o.d.o.*, pracodawca może wyznaczyć administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony danych osobowych (chyba, że sam wykonuje te czynności). Szczegółowe kwestie dotyczące: 1) sposobów prowadzenia i zakresu dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, 2) podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, 3) wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych określa Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dn. 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*[13]. Załącznik do tego rozporządzenia określa szczegółowe środki bezpieczeństwa, jakie mają być stosowane dla 3 poziomów bezpieczeństwa danych osobowych (podstawowego, podwyższonego i wysokiego). Należy przyjąć, że pracownik powinien zachować w tajemnicy konkretne środki bezpieczeństwa dla poziomu ochrony danych osobowych, na jakim operuje zgodnie z upoważnieniem pracodawcy i z jakimi został zapoznany przed przystąpieniem do wykonywania pracy umówionej.

Zakres czasowy ochrony danych osobowych oraz sposób ich zabezpieczenia

Ustawodawca w treści przepisu art. 39 ust. 2 *ustawy o.d.o.* nie określa granic czasowych trwania obowiązku zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Warto zauważyć, że w ustawodawstwie polskim istnieją regulacje dotyczące rozmaitych informacji chronionych, w przypadku których ustawodawca wprost lub pośrednio reguluje to zagadnienie w odpowiednich przypisach prawa. I tak, na przykład, w przypadku tak restrykcyjnie traktowanych przez prawo danych poufnych, jakimi są informacje niejawne (czyli informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania – art. 1 ust. 1 ustawy z dnia 5 sierpnia 2010 r. *o ochro-*

[13] Dz.U.2004.100.1024.

nie informacji niejawnych[14]), ustawodawca przewiduje co do zasady możliwość ustania stanu tajemnicy na zasadach określonych w art. 6 ust. 1–10 tej ustawy. Informacje niejawne podlegają bowiem ochronie w sposób określony ww. ustawie do czasu zniesienia lub zmiany klauzuli tajności na zasadach określonych w ustawie przez osobę nadającą klauzulę tajności, przy czym osoba ta, niejako z góry może określić konkretną datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności[15]. Jednocześnie ustawodawca wyraźnie wskazuje pewne szczególne kategorie informacji niejawnych podlegających na mocy wyraźnego postanowienia prawa ochronie bezterminowej (art. 7 ust. 1 ustawy *o ochronie informacji niejawnych*[16]). Inne rozwiązanie przyjęte jest z kolei w przepisach ustawy z dnia 29 sierpnia 1997 r. *Ordynacja podatkowa*[17]. Wprost zobowiązuje ona wymienione w niej wyraźnie kategorie pracowników objętych powinnością zachowania tajemnicy skarbowej do przestrzegania jej również po ustaniu zatrudnienia (zob. art. 294 § 1 i § 3 tej ustawy)[18]. Podkreślić warto w tym miejscu, że podobna formuła przyjęta był we wcześniejszych wersjach *ustawy o.d.o.* Z kolei w przypadku pracowników przetwarzających informacje stanowiące tajemnice przedsiębiorstwa, których przekazanie, ujawnienie lub wykorzystanie stanowi czyn nieuczciwej konkurencji w rozumieniu art. 11 ust. 1 ustawy z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*[19] powinność ich ochrony zachowuje aktualność przez okres trzech lat od ustania stosunku pracy, chyba że umowa stanowi inaczej albo ustał stan tajemnicy (art. 11 ust. 2 ww. ustawy). Odmiennie ustawa z dnia 29 sierpnia 1997 *Prawo bankowe*[20] określa w art. 104 ust. 1, że bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czyn-

[14] Dz.U.2016.1167 t.j.

[15] Szerzej zob. też. S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010, s. 98 i n.

[16] Zgodnie z art. 7 ust. 1 ustawy *o ochronie informacji niejawnych* chronione bez względu na upływ czasu, są (z pewnymi zastrzeżeniami z ust. 2 – JB): 1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych, jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności; 2) dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy; 3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

[17] Dz.U.2015.613 j.t. ze zm.

[18] Zgodnie z art. 294. § 1 *ordynacji podatkowej* do przestrzegania tajemnicy skarbowej obowiązani są: 1) pracownicy izb skarbowych; 1a) funkcjonariusze celni i pracownicy urzędów celnych oraz izb celnych; 2) wójt, burmistrz (prezydent miasta), starosta, marszałek województwa oraz pracownicy urzędów ich obsługujących; 3) członkowie samorządowych kolegiów odwoławczych, a także pracownicy biur tych kolegiów; 4) minister właściwy do spraw finansów publicznych oraz pracownicy tego ministerstwa; 5) osoby odbywające staż, praktykę zawodową lub studencką w urzędzie obsługującym ministra właściwego do spraw finansów publicznych lub w innych organach podatkowych, 6) przedstawiciele obcej władzy przebywający w siedzibach organów podatkowych, obecni w toku postępowania podatkowego lub obecni w toku czynności kontrolnych, w związku z wymianą informacji.

[19] Dz.U.2003.153.1503 j.t ze zm.

[20] Dz.U. 2015.128 j.t. ze zm.

ność wykonuje. Stan tajemnicy bankowej ma obejmować cały horyzont czasowy związany z dokonywaniem rozmaitych czynności, do który uprawnia bank ustawa. A zatem o ile w konkretnym przypadku stan tajemnicy bankowej może być długotrwały, to czy zasadne jest stwierdzenie, że stan ten jest nieograniczony w czasie? Jak w związku z tym stwierdził Sąd Najwyższy w wyroku z dn. 19 lutego 2010 r., IV CSK 428/09[21], przepis art. 104 ust. 1 ustawy z 1997 r. *Prawo bankowe* nie precyzuje, czy wymienione w nim podmioty obowiązane są do zachowania tajemnicy bankowej także po utracie określonego w nim statusu. Nie wskazuje też końcowego terminu związania tych podmiotów obowiązkiem zachowania tajemnicy. Zdaniem Sądu trzeba zatem uznać, że obowiązek ten jest bezterminowy. Zastosowanie odmiennego rozwiązania ograniczyłoby w sposób istotny efektywność ochrony beneficjentów tajemnicy bankowej. Konstatacja ta prowadzi do wniosku, że obowiązek zachowania tajemnicy bankowej spoczywa również na byłym pracowniku banku, a naruszenie przez niego tego obowiązku może uzasadniać odpowiedzialność odszkodowawczą banku. Obowiązek zachowania tajemnicy bankowej stanowi czynność powierzoną pracownikowi banku nie tylko na czas trwania stosunku pracy, ale i na okres po jego ustaniu. W takim ujęciu nie ma przeszkód do przyjęcia odpowiedzialności banku za szkodę spowodowaną ujawnieniem tajemnicy przez byłego pracownika[22].

W odniesieniu do kwestii wymiaru czasowego powinności zachowania tajemnicy danych osobowych i sposobów ich zabezpieczenie w literaturze zaznaczyły się dwa poglądy. Zgodnie z pierwszym nich, pomimo że analizowany przepis nie wskazuje wyraźnie obowiązku zachowania tajemnicy także po ustaniu upoważnienia, przyjąć należy, że omawiany obowiązek trwa także po tym fakcie, jako że ustawa nie przewiduje wprost ograniczenia czasowego tego obowiązku[23]. Zgodnie zaś z poglądem autora niniejszego opracowania należy podkreślić, że *ustawa o.d.o.* wyraźnie nakłada obowiązek zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia na podmioty określane jako „osoby, które zostały upoważnione do przetwarzania danych…". Pracownik, którego upoważnienie wygasło (np. w związku z upływem terminu, na jaki było wydane) lub zostało cofnięte przez pracodawcę, nie ma statusu osoby upoważnianej do przetwarzania danych osobowych. W konsekwencji, powinien być skreślony z ewidencji osób upoważnionych do przetwarzania danych osobowych u danego pracodawcy a pracodawca powinien dokonać stosownych czynności technicznych i organizacyjnych uniemożliwiających mu dostęp do danych w systemie informatycznym oraz/lub danych przetwarzanych w tradycyjnych zbiorach danych. Przypadek, w którym były pracownik, którego upoważnienie do przetwarzania danych osobowych ustało w związku z rozwiązaniem stosunku pracy, w dalszym ciągu dysponowałby zbiorem danych należącym do byłego pracodawcy należałoby traktować jak przetwarzanie danych w zbiorze przez osobę, która nie jest do tego uprawniona. W świetle art. 49 ust. 1 *ustawy o.d.o* stanowi to przestępstwo, którego sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia

[21] LEX nr 585878 – teza 3.

[22] O tajemnicy bankowej szerzej z uwzględnieniem tezy o braku jej ograniczenia w czasie zob. np. M. Siwiec, *Tajemnica bankowa w postępowaniu karnym*, Prokuratura i Prawo z 2003 r., nr 5, s.29–45.

[23] Zob. np. A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2004, s.260–261.

wolności do lat 2. Natomiast ustawodawca odrębnie penalizuje czyny mogące być łączone z przypadkami naruszeniem obowiązku zachowania danych osobowych w tajemnicy przez osobę upoważnioną do przetwarzania danych osobowych. I tak, zgodnie z art. 51 ust. 1 *ustawy o.d.o.* przestępstwo popełnia ten, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, zgodnie zaś z art. 52 *ustawy o.d.o.* przestępstwo popełnia ten, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Powyższe może stanowić argument na rzecz tezy istnieniu obowiązku zachowania w poufności danych osobowych i sposób ich zabezpieczenia wyłącznie w okresie, w którym pracownik legitymuje się ważnym upoważnieniem do ich przetwarzania wydanym przez pracodawcę – administratora danych osobowych.

Podsumowanie

1. Pracownik administrujący danymi osobowymi na podstawie upoważnienia pracodawcy zobowiązany jest do przestrzegania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia stosowanych u danego pracodawcy, jak jednej z tajemnic określonych w odrębnych przepisach (art. 39 ust. 2 *ustawy o.d.o.* w związku z art. 100 § 2 pkt. 5 k.p.). Zachowując te tajemnice, spełnia on wyrażoną ww. przepisie k.p. powinność pracowniczą, a praca przez niego wykonywana może być uznana za spełnioną należycie.

2. Pracowniczy obowiązek zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia przez pracownika przetwarzającego te dane w ramach wykonywania obowiązków ze stosunku pracy jest niezależny od tego, czy i jaką szkodę mogłoby wyrządzić pracodawcy ujawnienie tych danych podmiotom nieuprawnionym.

3. Obowiązek zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia ciąży na upoważnionym pracowniku na mocy *ustawy o.d.o.*, a więc niezależnie od podjęcia przez pracodawcę czynności zmierzających do zachowania ich poufności[24].

4. Obowiązek dostarczenia środków technicznych i informatycznych oraz obowiązek właściwego, zapewniającego poufność zorganizowania pracy pracowników administrujących danymi osobowymi spoczywa na pracodawcy, jako administratorze danych osobowych. Pracodawca w wykonaniu powinności wynikającej z art. 94 pkt. 1 k.p. ma obowiązek zapoznać pracownika upoważnionego z zakresem jego obowiązków i uprawnień w odniesieniu do przetwarzania danych osobowych oraz z zapewniającymi poufność sposobami wykonywania pracy umówionej na wyznaczonym stanowisku.

5. Należy rozważyć także przypadek, w którym dostęp do danych osobowych (albo informacje o sposobach ich zabezpieczenia) uzyskuje pracownik niedysponujący odpowiednim upoważnieniem pracodawcy – administratora danych osobowych. Przesłanką obowiązku zachowania ich w tajemnicy będą w tej sytuacji przepisy powszechnie obo-

[24] W literaturze wskazuje się, że tajemnica osoby upoważnionej do przetwarzania danych osobowych to tajemnica publicznoprawna, ustanowiona w drodze ustawy (wyznaczającej zakres informacji objętych ochroną) – zob. J. Barta..., *Komentarz do art. 39…*, tamże**,** dostęp z 5 lutego 2016 r. – i przytaczana tam literatura przedmiotu. Patrz też M. Madej, tamże, s. 30.

wiązujące[25]. W literaturze przyjmuje się, że powinność ochrony informacji poufnych pracodawcy wyprowadzona być może z obowiązku dbania o dobro zakładu pracy i zasady lojalności pracownika względem pracodawcy. Ze względu na wartość ekonomiczną informacji poufnych (np. zgromadzonych w bazach danych osobowych klientów) obowiązek ich ochrony łączony być może z obowiązkiem poszanowania mienia pracodawcy[26]. Obowiązki te ciążą na każdym pracowniku niezależnie od rodzaju pracy umówionej i niezależnie od faktu istnienia lub braku upoważnienia do dostępu do danych osobowych. W konkretnym przypadku dane osobowe będące w dyspozycji pracodawcy traktowane być mogą zatem jako tajemnica pracodawcy w rozumieniu art. 100 § 2 pkt 4 k.p. (… czyli informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę). W przypadku pracodawców – przedsiębiorców stanowić one mogą tajemnicą przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*[27]. Można je także w konkretnym przypadku uznać za wchodzące do domeny jednej z tajemnic sektorowych (np. tajemnicy bankowej) albo też, przy spełnieniu odpowiednich przesłanek, zakwalifikować jako informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*.

6. Zakresy pojęć: tajemnicy danych osobowych i sposobów ich zabezpieczania oraz tajemnicy pracodawcy, tajemnicy przedsiębiorstwa, tajemnicy informacji niejawnych czy innych tajemnic reglamentowanych prawnie mogą niejednokrotnie krzyżować się lub w węższym lub szerszym zakresie pokrywać się ze sobą[28]. W konsekwencji w konkretnym przypadku pracodawca może dążyć do zabezpieczenia swoich interesów związanych z bezpieczeństwem danych osobowych przetwarzanych w związku ze swoją dzielnością także przez zastosowanie takich „narzędzi", jak umowy o zakazie konkurencji w trakcie trwania stosunku pracy i po jego ustaniu (art. 101^1 § 1–art. 101^4 k.p.) lub klauzule poufności (na podstawie przepisów ustawy z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*).

7. W literaturze podejmowane są próby zaliczenia tajemnicy danych osobowych oraz sposobów ich zabezpieczenia to szerszych kategorii pojęciowych. W przeszłości wskazywałem, że nie ma uzasadnienia do określania jej jako „tajemnicy pracowniczej", w sytuacji w której adresatem tej powinności są osoby upoważnione do przetwarzania danych a nie wyłącznie upoważnione osoby przetwarzające te dane w ramach wykonywania obowiązków ze stosunku pracy[29]. Ponieważ więc dane te mogą być przetwarzane przez osoby pozostające w różnych stosunkach zatrudnienia – bardziej adekwatne jest okre-

---

[25] Zob. M. Madej, tamże, s. 29.

[26] Zob. M. Derlacz-Wawrowska, *Ochrona informacji poufnych pracodawcy w indywidualnym i zbiorowym prawie pracy*, Warszawa 2015, s. 87.

[27] Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności – art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*.

[28] Zob. np. wyrok NSA Warszawa z dn. 16 kwietnia 2014 r. , I OSK 2339/13, LEX nr 1574629, teza 1, zgodnie z którą „*pojęcie danych osobowych klienta banku mieści się w pojęciu informacji i tajemnicy bankowej. Do danych osobowych klienta banku należy zaś numer rachunku bankowego tej osoby*".

[29] J. Borowicz, *Sytuacja prawna pracownika przetwarzającego dane osobowe*…, tamże, s. 20.

ślanie jej w literaturze jako tajemnicy funkcyjnej[30]. W przypadku przetwarzania danych osobowych przez upoważnionego pracownika właściwe byłoby określenie jej mianem tajemnicy stanowiskowej, jako że nie każdy pracownik będzie uzyskiwał do niej dostęp – a jedynie ten, który wykonując na danym stanowisku pracę określonego rodzaju musi w ocenie pracodawcy administrować danymi osobowymi[31]. Należy zgodzić się, że chybione jest klasyfikowanie tajemnicy danych osobowych i sposobów ich zabezpieczenia jako tajemnicy zawodowej, w sytuacji gdy instytucja upoważnienia nie została również powiązana z wykonywaniem określonych zawodów[32]. Pamiętać też należy o nieostrości pojęcia tajemnicy zawodowej, grożącej obejmowaniem zakresem obowiązku jej ochrony praktycznie każdego pracownika, który w celach zarobkowych stale wykonuje jakikolwiek wymagający odpowiednich kwalifikacji (wiedzy i umiejętności) zespół czynności wyodrębnionych w wyniku społecznego podziału pracy[33]. W przypadku pracowników w rozumieniu k.p. należałoby postulować ograniczenie stosowania pojęcia tajemnicy zawodowej do przypadku tych z nich, którzy dysponują szczególnymi uprawnieniami zawodowymi, z którymi na mocy wyraźnego przepisu prawa powiązany jest obowiązek zachowania tajemnicy zawodowej . Są to osoby wykonujące jeden z zawodów zaufania publicznego w ramach stosunku pracy, zobowiązane do zachowania tajemnicy określanej w przepisach prawa wprost jako „zawodowa”[34]. Tak, na przykład, radca prawny zgodnie z art. 3 ust. 3–5 ustawy z dnia 6 lipca 1982 r. *o radcach prawnych*[35] jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej, zaś jego obowiązek zachowania tajemnicy zawodowej nie może być ograniczony w czasie. Radca prawny co do zasady nie może być zwolniony z obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę. Należy oczywiście zgodzić się, że przy uwzględnieniu prawnie zdefiniowanego przedmiotu danego zawodu zaufania publicznego, do domeny tajemnicy zawodowej w konkretnym przypadku mogą wejść także dane osobowe osób, które wykonawca zawodu powziął w związku z udzielaniem usługi zawodowej.

---

[30] Zob. J. Barta ..., *Komentarz do art. 39…*, tamże**,** dostęp z 9 lutego 2016 r. – i przytaczana tam literatura przedmiotu.

[31] J. Borowicz, *Pracowniczy obowiązek przestrzegania tajemnicy określonej w odrębnych przepisach (art. 100 § 2 pkt 5 k.p.),* PiZS z 2013 r., nr 9, s. 30–31.

[32] zob. J Barta ..., *Komentarz do art. 39…*, tamże**,** dostęp z 9 lutego 2016 r.

[33] Zob. np. definicja zawodu zawarta w rozporządzeniu Ministra Gospodarki i Pracy z dnia 27 kwietnia 2010 r. *w sprawie klasyfikacji zawodów i specjalności dla potrzeb rynku pracy oraz zakresu jej stosowania,* Dz.U.10.82.537.

[34] J. Borowicz, *Pracowniczy obowiązek…*, tamże.

[35] Dz.U.2016.233 t.j.

Summary
Characteristics of Employee's Duty to Protect Personal Data

Pursuant to Article 100 § 2 item 5 of the Labour Code dated 26 June 1974 an employee is required to observe confidentiality laid down under separate statutory provisions. This obligation covers a worker who, by virtue of the pursuit of a particular type of work or by virtue of the place where the work is exercised, has access to information of the kind covered by the obligation of secrecy laid down in separate provisions. One of the cases of confidentiality protected by law under separate provisions is the confidentiality of personal data and the ways of their protection. The obligation of confidentiality by persons authorised to process personal data is based on Article 39(2) of the Data Protection Act of 29 August 1997. The employer, acting as the administrator of personal data, gives an individually appointed employee by name the authorisation to process personal data. In the authorisation the employer shall specify the following: 1) types of personal data to which a given employee shall have access, 2) means of the processing of personal data to be fulfilled by a given employee. The employee authorised to process personal data shall be bound by the obligation to keep the data and the ways of their protection used by a given employer secret.

Keywords: employee, employee's duty of confidentiality, personal data, person authorized to process personal data, confidentiality of personal data