10.17951/g.2020.67.1.137-147

ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. LXVII, 1 SECTIO G 2020

Wyższa Szkoła Ekonomii i Innowacji w Lublinie

ŁUKASZ WOJCIECHOWSKI
lukasz.wojciechowski@wsei.lublin.pl
ORCID: 0000-0002-9403-6412

Przedsiębiorca w dobie przemian związanych z nowymi uregulowaniami prawnymi ochrony danych osobowych w świetle nowelizacji ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy

Entrepreneur Confronted with Changes Related to New Legal Regulations Concerning Protection of Personal Data in the Light of the Amendment to the Act of 26 June 1974 – Labour Code

WPROWADZENIE

Prowadzenie działalności gospodarczej wiąże się z licznymi obowiązkami, jakie zostały nałożone na przedsiębiorców. Jest to spowodowane reglamentowaniem przez państwo wytwarzania i sprzedaży niektórych dóbr i usług, jak również koniecznością budowy transparentnego systemu pobierania danin. Organy państwowe mają też obowiązek zapewnienia ochrony realizacji praw i wolności osób fizycznych. Realizacja tego obowiązku w praktyce wiąże się z koniecznością kreowania i udoskonalania systemu ochrony danych osobowych. Oznacza to ochronę informacji o osobach, które zostały lub mogą zostać zidentyfikowane właśnie z wykorzystaniem tych informacji. Jedną z priorytetowych kategorii danych osobowych przetwarzanych przez przedsiębiorców są dane osobowe pracowników. Metody i środki ich zabezpieczania powinny być dostosowane do szerokiego spektrum czynników, przede wszystkim do liczebnego stanu zatrudnienia w danym podmiocie.

Celem artykułu jest analiza obowiązku prawnego przedsiębiorcy w zakresie przetwarzania danych osobowych pracowników oraz kandydatów do pracy. Zakres

danych osobowych, co do których istnieje legalna przesłanka ich przetwarzania w postaci przepisu prawa, uległ zmianie wraz z wejściem w życie ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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)[1], na mocy której wprowadzono zmiany w ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy[2]. W opracowaniu poddano weryfikacji hipotezę badawczą, iż zmiany w prawie pracy przyczyniły się do zwiększenia bezpieczeństwa i bardziej efektywnej ochrony prywatności pracowników, których dane przetwarzają pracodawcy. Do przygotowania artykułu zastosowano trzy metody badawcze. Pierwsza z nich to metoda instytucjonalno-prawna, która umożliwiła analizę aktów normatywnych regulujących poruszone zagadnienia. Druga to analiza czynnikowa, która umożliwiła wyodrębnienie istotnych aspektów w zakresie przetwarzania danych osobowych pracowników i kandydów do pracy przez przedsiębiorcę. Trzecią zastosowaną metodą jest metoda komparatystyczna, za pomocą której zostały porównane zakresy przetwarzanych danych osobowych pracowników, które pracodawca mógł przetwarzać przed reformą systemu i po wejściu w życie nowych uregulowań prawnych.

PRZEDSIĘBIORCA W DOBIE ZMIAN – REFORMA SYSTEMU OCHRONY DANYCH OSOBOWYCH W LATACH 2016–2018

Reforma systemu ochrony danych osobowych została wprowadzona w Polsce w związku ze zmianami w prawie wspólnotowym. Nowe regulacje weszły w życie w formie 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[3]. Było to odejście od dotychczasowego modelu autonomicznej ochrony realizowanej przez poszczególne państwa Unii Europejskiej poprzez implementację dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[4]. W Polsce uchwalona została nowa ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[5], nie był to jednak akt prawny implementujący

[1] Dz.U. 2019, poz. 730.
[2] Dz.U. 2019, poz. 1040.
[3] Dz.Urz. L 119, 4.05.2016.
[4] Dz.Urz. WE L 281, 23.11.1995.
[5] Dz.U. 2018, poz. 1000.

nowe przepisy prawa Unii Europejskiej, ponieważ nie wymagały one implementacji z uwagi na swoją rangę. W ustawie wskazano natomiast rozwiązania szczegółowe, np. w rozporządzeniu Parlamentu Europejskiego i Rady usankcjonowano nowy system składania skarg na podmioty, które naruszają zasady ochrony danych osobowych, a w ustawie wskazano organ (Prezesa Urzędu Ochrony Danych Osobowych), do którego w Polsce należy kierować skargi.

Warto podkreślić, że Grupa Robocza Art. 29 (obecnie funkcjonująca jako Europejska Rada Ochrony Danych) podczas merytorycznych prac nad przepisami rozporządzenia 2016/679 zdecydowała się zastosować rozwiązania zawarte w Międzynarodowej Normie ISO/IEC 27001. Oznacza to wskazanie trzech obszarów priorytetowych: poufności, dostępności i integralności, co w przypadku podmiotów przetwarzających dane osobowe oznacza nie tylko konieczność ich ochrony przed nieuprawnionym dostępem, lecz także zapewnienie dostępu do danych i zabezpieczenie przed wprowadzaniem nieuprawnionych zmian. Takie podejście dało jednocześnie przewagę we wdrażaniu nowych rozwiązań podmiotom, w których procedury wewnętrzne również zostały przygotowane na podstawie Normy, w Polsce opublikowanej obecnie jako PN-ISO/IEC 27001:2014-12. Atutem wprowadzenia takich procedur jest otrzymanie sprawdzonych i efektywnych narzędzi w zakresie audytu[6], co pozwala realizować wymagania zawarte w rozporządzeniu 2016/679 – „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania" (art. 32 ust. 1 lit. d).

Ponadto rozporządzenie 2016/679 zawiera obszerną preambułę (173 motywy), w której znajduje się opis istoty nowych regulacji. Stanowi ona istotną przesłankę podczas dokonywania wykładni nowych przepisów prawa[7]. Przepisy te mają charakter uniwersalny i odnoszą się zarówno do instytucji publicznych, jak i do przedsiębiorstw. Jednocześnie analiza rozporządzenia prowadzi do konkluzji, że w przypadku niektórych obowiązków i rozwiązań szczegółowych przyjęto wyraźne rozróżnienie pomiędzy podmiotami publicznymi a firmami prywatnymi. W przypadku niektórych obowiązków przedsiębiorcy zyskali większą autonomię, przy jednoczesnym ich obligatoryjnym charakterze dla instytucji publicznych. Taka sytuacja występuje przede wszystkim w dwóch obszarach.

Pierwszy z nich to powoływanie inspektora ochrony danych (art. 37 rozporządzenia 2016/679). Przed 25 maja 2018 r., czyli przed zakończeniem okresu przejściowego i rozpoczęciem bezwzględnego obowiązywania rozporządzenia,

---

[6] E. Wolska, *Audyt zgodności z normą ISO/IEC 27001:2005*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2012, nr 7, s. 88.

[7] K. Morawska, *Rola oraz status prawny motywów preambuły ogólnego rozporządzenia o ochronie danych – klucz do wykładni przepisów nowego prawa unijnego*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 25.

funkcja ta miała nazwę „administrator bezpieczeństwa informacji", a wyznaczenie osoby na to stanowisko miało charakter fakultatywny tak dla podmiotów publicznych, jak i dla firm prywatnych. W ostatnim etapie funkcjonowania systemu w poprzedniej formie próbowano jedynie tworzyć system zachęt do powoływania administratora, np. oferując w zamian odstąpienie od obowiązku rejestrowania niektórych zbiorów danych. Obecnie, poza precyzyjnie wskazanymi wyjątkami, powoływanie inspektora w dalszym ciągu jest autonomiczną decyzją przedsiębiorcy, natomiast w przypadku podmiotów publicznych ma to charakter obligatoryjny. Takie uregulowanie tego zagadnienia prawdopodobnie nie było motywowane chęcią nadania przedsiębiorcom większych uprawnień w sferze decyzyjnej. Wynikało zaś z potencjalnych trudności z powołaniem inspektora w jednoosobowych działalnościach gospodarczych i niektórych podmiotach sektora MŚP.

Drugi obszar to możliwość przetwarzania danych osobowych z uwagi na to, że „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" (art. 6 ust. 1 lit. f rozporządzenia 2016/679). Jest to jedna z legalnych przesłanek przetwarzania danych osobowych, jednak nie ma ona zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. W tym przypadku można mówić o realnym dostosowaniu nowych uregulowań prawnych do funkcjonowania firm prywatnych. Twórcy zmian wzięli pod uwagę, że w przypadku instytucji publicznych trudno jest mówić o prawnie uzasadnionych interesach, ponieważ ich głównym zadaniem jest wykonywanie zadań publicznych. Jednocześnie sytuacja jest inna w przypadku przedsiębiorców, którzy abstrahując od szerokiego katalogu przesłanek aksjologicznych w przypadku niektórych z nich, kierują się również w codziennych działaniach chęcią zysku. Jedną z najczęściej występujących okoliczności, w których przedsiębiorcy powołują się na prawnie uzasadniony interes, jest instalacja monitoringu wizyjnego na terenie siedziby firmy prywatnej. Wizerunek osób fizycznych, który zostaje zarejestrowany za pomocą aparatury, jest daną osobową. Gdyby nie stworzono przedstawionej przesłanki legalnego przetwarzania danych, to rejestrowanie obrazu monitoringu wizyjnego stałoby w sprzeczności z przepisami rozporządzenia 2016/679, nie byłoby bowiem możliwe uzyskanie zgody od wszystkich osób, które znalazły się w polu kamer. Nie istnieje także przepis prawa, na który przedsiębiorcy mogliby się powoływać, wskazując jako przesłankę legalizującą do przetwarzania danych osobowych monitoringu wizyjnego. W tej sytuacji prawnie uzasadniony interes w postaci zapewnienia bezpieczeństwa osób i mienia jako przesłanka legalizująca jest trafnym rozwiązaniem.

Przedstawione różnice w fakultatywnym i obligatoryjnym charakterze wykonywania niektórych czynności przez administratorów ze sfery budżetowej i administratorów-przedsiębiorców wskazywać mogą na liberalne podejście twórców reformy systemu ochrony danych osobowych do tych drugich. Warto jednak podkreślić, iż przedsiębiorcy nie zawsze są w uprzywilejowanej sytuacji w zakresie przetwarzania danych osobowych. Wynika to przede wszystkim z doświadczenia przedstawicieli instytucji publicznych, które umożliwia efektywną realizację zadań. Przykładem w tym zakresie jest analiza ryzyka, która miała już wcześniej charakter obligatoryjny dla podmiotów publicznych. Wynikało to z obowiązku wprowadzenia w tych instytucjach kontroli zarządczej na podstawie art. 68–71 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[8]. Obecnie wszystkie podmioty, w których w ramach wykonywanej działalności przetwarzane są dane osobowe, mają obowiązek przeprowadzania analizy ryzyka. Przedsiębiorcy, z wyjątkiem tych, którzy – jak wskazano wcześniej – wprowadzili procedury oparte na Normie PN-ISO/IEC 27001:2014-12 (lub innych), w większości przypadków nie mieli do tej pory obowiązku prowadzenia analizy ryzyka w żadnym zakresie. Pracownicy podmiotów sfery budżetowej mają też na ogół większe doświadczenie w udostępnianiu informacji[9]. W sformalizowanych strukturach (np. w urzędach) łatwiej jest również wypełniać tzw. obowiązek informacyjny (art. 13 i 14 rozporządzenia 2016/679), polegający na informowaniu osób, których dane dotyczą, m.in. o tym, kto jest administratorem ich danych oraz o możliwości złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych[10].

PRZETWARZANIE DANYCH OSOBOWYCH PRACOWNIKÓW – NOWELIZACJA USTAWY Z DNIA 26 CZERWCA 1974 R. – KODEKS PRACY

Przetwarzanie danych osobowych pracowników to specyficzny obszar związany z funkcjonowaniem wszystkich podmiotów, które są administratorami danych. Pojawiają się wątpliwości związane m.in. z zasadnością wypełniania obowiązku informacyjnego w stosunku do pracowników przedsiębiorstwa z uwagi na to, że większość z nich uzyskała te informacje już wcześniej. Wśród specjalistów w zakresie ochrony danych osobowych odbywa się także dyskusja na temat granic ingerencji przedsiębiorcy w prywatność pracownika, np. poprzez monitorowanie czynności, jakie wykonuje na swoim stanowisku pracy, włącznie z przeglądaniem

[8] Dz.U. 2019, poz. 869.

[9] P. Fajgielski, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007, s. 101–102.

[10] M. Gumularz, M. Kawecki, *Prawo do poinformowania w przypadku zbierania danych od osoby, której dane dotyczą*, [w:] *Realizacja praw osób, których dane dotyczą, na podstawie RODO*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 96.

służbowej korespondencji mailowej. Pracownicy bardzo często odczuwają w takich sytuacjach dyskomfort[11].

W pierwszym etapie realizacji reformy ochrony danych osobowych w Polsce skupiono się przede wszystkim na zmianach instytucjonalnych i stworzeniu systemów umożliwiających podmiotom przetwarzającym dane osobowe realizację przepisów rozporządzenia 2016/679, m.in. zgłaszanie naruszeń bezpieczeństwa w ciągu 72 godzin od uzyskania informacji o zdarzeniu oraz rejestrowanie inspektorów ochrony danych. Dopiero w dalszej kolejności zintensyfikowano prace nad nowelizacją 168 aktów prawnych w celu dostosowania funkcjonujących w państwie procedur do rozporządzenia. Zmiany nastąpiły po wejściu w życie wskazanej wcześniej ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679. Jednym z aktów prawnych, w którym wprowadzono zmiany, jest ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy[12]. Nowelizacja ustawy była niezbędna, ponieważ zarówno przed reformą systemu ochrony danych osobowych, jak i po wprowadzeniu zmian przesłanką legalizującą przetwarzanie danych osobowych pracowników było odwołanie się do przepisów kodeksu (art. 22^1). Katalog danych, które powołując się na ten przepis, pracodawca mógł pozyskiwać od kandydata do pracy, zawierał następujące elementy:

- imię (imiona) i nazwisko,
- imiona rodziców,
- datę urodzenia,
- miejsce zamieszkania (adres do korespondencji),
- wykształcenie,
- przebieg dotychczasowego zatrudnienia.

Oznaczało to, że bez wyrażenia oddzielnej, niedorozumianej zgody kandydata do pracy pracodawca nie mógł pozyskać od niego danych kontaktowych. Po zmianach istnieje już taka możliwość, lecz zrezygnowano z gromadzenia podczas rekrutacji imion rodziców. W tym przypadku konsekwencją stało się nowe rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 18 czerwca 2019 r. zmieniające rozporządzenie w sprawie świadectwa pracy[13]. Zawiera ono nowy wzór świadectwa pracy, w którym nie ma już imion rodziców. Pracodawca nie może również wymagać od kandydata podania adresu zamieszkania (adresu do korespondencji). Zastąpienie adresu danymi kontaktowymi należy uznać za zmianę, która dostosowuje proces rekrutacji do współczesnych standardów. Pozostałe istotne informacje znalazły się w katalogu danych, które są pozyskiwane na

[11] K. Michalski, *Konflikty interesów związane z bezpieczeństwem danych osobowych i ochroną prywatności w społeczeństwie cyfrowym*, „Zeszyty Naukowe WSIZiA" 2017, z. 3(40), s. 56–58.

[12] Dz.U. 2019, poz. 1040.

[13] Dz.U. 2019, poz. 1197.

potrzeby zakładu pracy od osób zatrudnionych. Pracodawca może obecnie żądać od pracownika:

- adresu zamieszkania,
- numeru PESEL (w przypadku jego braku – rodzaju i numeru dokumentu potwierdzającego tożsamość),
- innych danych osobowych pracownika, a także danych osobowych dzieci pracownika i innych członków jego najbliższej rodziny (jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy),
- informacji o wykształceniu i przebiegu dotychczasowego zatrudnienia (jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie).

Ustawodawca przewidział sytuację, w której wobec pracodawców mogą pojawić się nowe obowiązki wynikające z odrębnych aktów normatywnych. Stąd też mowa jest o „innych danych osobowych pracownika", co pozwoli uniknąć konieczności dalszych nowelizacji Kodeksu pracy. Przedsiębiorca gromadzi dane pracowników, które są przez nich udostępniane w formie oświadczenia, ma jednak możliwość zażądania dowodów w sprawie (np. jeżeli pracownik deklaruje uzyskanie stopnia naukowego doktora, to pracodawca może zażądać dostarczenia dyplomu, na którym zostało to potwierdzone).

Warto podkreślić, że katalog danych osobowych kandydata do pracy lub pracownika, które mogą być przetwarzane w zakładzie pracy, jest bardzo precyzyjny i nie pozostawia znaczącego pola do interpretacji. Daje to gwarancję lepszego zabezpieczenia praw osób fizycznych. Zdarza się bowiem, że legalna przesłanka przetwarzania danych osobowych, jaką jest przepis prawa, jest nadużywana i administratorzy powołują się na nią w sytuacji, w której przepisy nie są precyzyjne (administratorzy dokonują ich samodzielnej wykładni, interpretując je na swoją korzyść)[14].

W znowelizowanym Kodeksie pracy uporządkowano także kwestię przetwarzania szczególnych kategorii danych pracowników. Przed realizacją reformy systemu ochrony danych osobowych takie dane określano mianem „wrażliwych". Obecnie zalicza się do nich dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych. Zabrania się też przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby (art. 9 ust. 1 rozporządzenia 2016/679). Jeżeli pracodawca chce przetwarzać szczególne kategorie danych kandydata do pracy lub pracownika, to podanie tych danych musi wynikać z inicjatywy osób, których dane dotyczą. Jednocześnie,

[14] P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 27–28.

zgodnie z art. 22^{1a} § 2 Kodeksu pracy, „brak zgody […] lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę". Pracodawca może przetwarzać dane biometryczne pracownika, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony. W Kodeksie pracy usankcjonowano również obowiązek nadania pisemnych upoważnień pracownikom, którzy będą przetwarzali szczególne kategorie danych. Pomimo tego, że nadawanie upoważnień jest powszechnie stosowaną dobrą praktyką w instytucjach publicznych, wielu przedsiębiorców nie stosuje takiego rozwiązania. Stąd stworzenie obowiązku prawnego w tym zakresie należy uznać za zasadne, w tym z uwagi na wymiar edukacyjny, szczególnie w przypadku podmiotów sektora MŚP, w których stosowanie procedur ochrony danych osobowych stanowi często obszar deficytowy[15].

Nowym regulacjom poddany został jeszcze monitoring wizyjny w zakładach pracy. Rejestrowanie wizerunku pracownika jest przetwarzaniem jego danych osobowych. Warto jednak pamiętać, że pracodawca powinien również zapewnić bezpieczeństwo osób i mienia. W niektórych przypadkach może także kontrolować produkcję lub chronić informacje, których ujawnienie mogłoby narazić go na szkodę. Stąd pojawiła się inicjatywa uregulowania tego zagadnienia w prawie pracy. Ostatecznie przyjęto rozwiązanie, że monitoring wizyjny nie może być instalowany w pomieszczeniach udostępnianych zakładowej organizacji związkowej (art. 22^2 § 1^1 Kodeksu pracy). Ponadto monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że jego stosowanie w tych pomieszczeniach jest niezbędne do realizacji wymienionych wcześniej celów pracodawcy i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Zgodę na takie zastosowanie monitoringu musi wyrazić organizacja związkowa, a jeżeli nie ma jej w zakładzie pracy, to muszą to zrobić przedstawiciele pracowników w trybie przyjętym u danego pracodawcy (art. 22^2 § 2 Kodeksu pracy). Przedstawione regulacje dotyczą kwestii przetwarzania danych osobowych pracowników, dlatego nie można ich stosować jako podstawy prawnej rejestrowania wizerunku osób postronnych. Jak wskazano wcześniej, przedsiębiorcy są w tym przypadku jednak uprzywile-

[15] Ł. Wojciechowski, *Realizacja obowiązku prawnego w zakresie bezpieczeństwa informacji i ochrony danych osobowych jako dysfunkcjonalny obszar funkcjonowania podmiotów sektora MŚP w Polsce*, [w:] *Mechanizmy wspomagania sektora MŚP*, red. M. Stefański, Lublin 2017, s. 198–199.

jowani w stosunku do podmiotów publicznych, ponieważ mogą jako przesłankę legalnego przetwarzania tych danych wskazać prawnie uzasadniony interes realizowany przez administratora.

Stosowanie nowych przepisów Kodeksu pracy w praktyce ma istotne znaczenie z uwagi na fakt, że przedsiębiorca niestosujący wskazanych regulacji może spotkać się z zarzutem naruszania przepisów rozporządzenia 679/2016. Takie działanie wiąże się z możliwością nałożenia na administratora danych osobowych wysokich kar finansowych, do tej pory niespotykanych w polskim systemie prawnym. Zgodnie z art. 83 rozporządzenia maksymalna wysokość kary wynosi 20 mln euro lub do 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa). W Polsce podmiotem nakładającym kary jest Prezes Urzędu Ochrony Danych Osobowych. W rozporządzeniu określono także szerokie spektrum przesłanek, które powinny zostać uwzględnione w przypadku nakładania kary (m.in. kategorie danych osobowych, których dotyczyło naruszenie). Pracownik zyskał też bardziej efektywne narzędzie w zakresie ochrony swoich praw i wolności. Od 25 maja 2018 r. istnieje bowiem możliwość bezpłatnego złożenia skargi (drogą elektroniczną, pocztą tradycyjną lub osobiście, dostarczając skargę w formie pisemnej). Podmiotem, który rozpatruje skargi, również jest Prezes Urzędu Ochrony Danych Osobowych.

PODSUMOWANIE

Przedstawione rozważania pozwoliły na pozytywną weryfikację hipotezy badawczej, iż zmiany w prawie pracy przyczyniły się do zwiększenia bezpieczeństwa i bardziej efektywnej ochrony prywatności pracowników, których dane przetwarzają pracodawcy. Uzasadnienie pozytywnej weryfikacji hipotezy wymaga sformułowania kilku konkluzji. Pierwsza z nich dotyczy sytuacji przedsiębiorcy w dobie przemian związanych z nowymi uregulowaniami prawnymi ochrony danych osobowych. Warto zwrócić uwagę, że konieczność wprowadzania nowych procedur i rozwiązań stanowiła de facto dodatkowy obowiązek dla przedsiębiorców, co mogło spotkać się z niezrozumieniem i brakiem akceptacji. Przetwarzanie danych osobowych ma jednak obecnie tak istotne znaczenie w wymiarze globalnym, że skierowanie do tego obszaru kapitału ludzkiego i środków finansowych bez wątpienia zaprocentuje w przyszłości, m.in. pozwoli przedsiębiorcom uniknąć zagrożeń, które mogłyby wiązać się z utratą znaczących środków finansowych. Jednocześnie beneficjentami zmian są osoby fizyczne, w tym pracownicy przedsiębiorstw. Dzięki ogólnonarodowej dyskusji na temat reformy systemu ochrony danych osobowych, której punkt kulminacyjny miał miejsce w 2018 r., stali się oni bardziej świadomi swoich praw. Osoby rekrutujące się do pracy i pracownicy zaczęli stopniowo wymagać od przedstawicieli zakładów pracy poszanowania ich prywatności oraz przetwarzania ich danych osobowych w bezpieczny sposób.

Nowe przepisy prawa pracy są dostosowane do współczesnych potrzeb i metod działania przedsiębiorców. Umożliwiają pozyskanie potrzebnych danych osobowych bez rozbudowanych procedur biurokratycznych. Zwrócono m.in. uwagę na fakt, że podczas rekrutacji na stanowisko pracy istotne znaczenie będzie miał kontakt telefoniczny lub za pośrednictwem poczty elektronicznej, nie będzie natomiast konieczne wysyłanie dokumentów w formie papierowej na adres korespondencyjny. Precyzyjnej regulacji poddano również trudne zagadnienia związane z rozwojem nowoczesnych technologii – przetwarzanie danych biometrycznych, a także monitoring wizyjny. W przypadku tego drugiego nie jest to oczywiście rozwiązanie innowacyjne, ale należy pamiętać, że urządzenia rejestrujące stały się bardziej dostępne i jednocześnie są bardziej powszechne z uwagi na niższe ceny.

Ostatnią konkluzję stanowi postulat prowadzenia dalszych badań naukowych nad problematyką funkcjonowania przedsiębiorstw w zakresie realizacji ochrony danych osobowych. Jest to zagadnienie, które ciągle się rozwija i wymaga pogłębionej interdyscyplinarnej dyskusji akademickiej. Ciągle nie wypracowano bowiem optymalnych rozwiązań, a ujawniane statystyki naruszeń bezpieczeństwa danych są wykładnikiem tego, jak dużo jest jeszcze w tym zakresie do zrobienia.

BIBLIOGRAFIA

Literatura

Fajgielski P., *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007.

Gumularz M., Kawecki M., *Prawo do poinformowania w przypadku zbierania danych od osoby, której dane dotyczą*, [w:] *Realizacja praw osób, których dane dotyczą, na podstawie RODO*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.

Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Michalski K., *Konflikty interesów związane z bezpieczeństwem danych osobowych i ochroną prywatności w społeczeństwie cyfrowym*, „Zeszyty Naukowe WSIZiA" 2017, z. 3(40).

Morawska K., *Rola oraz status prawny motywów preambuły ogólnego rozporządzenia o ochronie danych – klucz do wykładni przepisów nowego prawa unijnego*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017.

Wojciechowski Ł., *Realizacja obowiązku prawnego w zakresie bezpieczeństwa informacji i ochrony danych osobowych jako dysfunkcjonalny obszar funkcjonowania podmiotów sektora MŚP w Polsce*, [w:] *Mechanizmy wspomagania sektora MŚP*, red. M. Stefański, Lublin 2017.

Wolska E., *Audyt zgodności z normą ISO/IEC 27001:2005*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2012, nr 7.

Akty prawne

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz.Urz. WE L 281, 23.11.1995).

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 (Dz.Urz. L 119, 4.05.2016).
Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 18 czerwca 2019 r. zmieniające rozporządzenie w sprawie świadectwa pracy (Dz.U. 2019, poz. 1197).
Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz.U. 2019, poz. 1040).
Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2019, poz. 869).
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).
Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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) (Dz.U. 2019, poz. 730).

SUMMARY

The aim of the article was to analyze legal aspects of the functioning of the companies in relation with changes in labour law introduced due to the fact that the Act of 21 February 2019 on changes to some acts because of the appliance to the General Data Protection Regulation (GDPR) came into force. The implementation of new legal regulations is connected with the necessity to change the procedures of recruiting new employees. Furthermore, the regulation deals with the processing of the personal data of people working in the company. The issue is worth analyzing because of the wide spectrum of threats to companies which do not abide by new regulations. These threats are, among others, financial penalties which are granted by the President of the Personal Data Protection Office.

Keywords: labour law; GDPR; entrepreneurship

STRESZCZENIE

Celem artykułu była analiza prawnych aspektów funkcjonowania przedsiębiorstw w związku ze zmianami w prawie pracy, które zostały wprowadzone w związku z wejściem w życie ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia ogólnego o ochronie danych osobowych (RODO). Realizacja nowych uregulowań prawnych wiąże się z koniecznością zmiany procedur rekrutacji nowych pracowników. Uporządkowany został także obszar przetwarzania danych osobowych osób już zatrudnionych w przedsiębiorstwach. Zagadnienie to ma istotne znaczenie z uwagi na szerokie spektrum zagrożeń dla funkcjonowania firm w przypadku niestosowania w praktyce nowych przepisów. Wśród nich wskazać należy m.in. kary finansowe, które może nałożyć Prezes Urzędu Ochrony Danych Osobowych.

Słowa kluczowe: prawo pracy; RODO; przedsiębiorczość