DOI: 10.31648/sp.10094

Stanislaw Hady-Głowiak
Uniwersytet Ekonomiczny w Katowicach
ORCID: 0000-0002-1060-6984
stanislawhg@gmail.com

Wybrane aspekty prawne oraz praktyczne dotyczące ochrony danych osobowych i związane z wykonywaniem pracy na odległość

Wstęp

Przedmiotem niniejszego artykułu jest problematyka ochrony danych osobowych związana z funkcjonowaniem pracy na odległość zgodnie z obowiązującymi przepisami prawnymi, począwszy od momentu wprowadzenia telepracy poprzez okres pandemii COVID-19 do czasu zmiany przepisów prawa pracy z uwzględnieniem wymogów wynikających z przepisów o ochronie danych osobowych w tym zakresie. Celem artykułu jest również próba odpowiedzi na pytanie, czy wykonywanie pracy w formie zdalnej stanowi szansę, czy zagrożenie dla pracodawcy w aspekcie skutecznego i efektywnego wykonywania zadań przez podległych pracowników adekwatnie do występujących ryzyk w cyberprzestrzeni. W artykule zanalizowano również rolę doradczą i monitorującą inspektora ochrony danych (dalej jako IOD) w instytucji w zapewnieniu warunków bezpiecznego świadczenia pracy na odległość adekwatnie do zagrożeń przy uwzględnieniu ciągłych zmian legislacyjnych, organizacyjnych, czy stosowanych narzędzi. Niniejszy tekst składa się z dwóch części i zakończenia. W pierwszym podrozdziale skupiono się na dotychczas obowiązujących przepisach regulujących zasady świadczenia pracy na odległość oraz na zmianach jakie wprowadziła nowelizacja kodeksu pracy. Przedstawione zostały również pewne elementy statystyk, wskazujące, jak kształtowało się wykonywanie pracy na odległość na przestrzeni lat oraz liczby zagrożeń w cyberprzestrzeni. W kolejnym podrozdziale poruszone zostały zagadnienia dotyczące problematyki bezpieczeństwa informacji i ochrony danych osobowych przy wykonywaniu pracy na odległość w praktyce jej funkcjonowania oraz podkreślono rolę IOD w przedmiotowym zakresie.

Pojęcie i ewolucja funkcjonowania pracy na odległość

Wykonywanie pracy poza siedzibą pracodawcy z wykorzystaniem urządzeń mobilnych nie stanowi *novum* w polskim porządku prawnym. Dotychczas narzędzie to było najczęściej wykorzystywane przez sektor prywatny, a zyskało na znaczeniu w sektorze publicznym podczas pandemii COVID-19. Nie w każdym przypadku praca musi być realizowana z poziomu zakładu pracy. Tam, gdzie praca nie wiąże się z koniecznością użytkowania skomplikowanej infrastruktury – maszyn i urządzeń, a jej efekty mogą być w szczególności przekazywane drogą elektroniczną, istnieje możliwość wykonywania zadań przykładowo z miejsca zamieszkania pracownika.

Szybki postęp techniczny i rozwój nowoczesnych technologii mają istotny wpływ na ochronę danych osobowych, umożliwiając z jednej strony swobodny przepływ tych danych i ich przetwarzanie na niespotykaną dotąd skalę, z drugiej zaś generując zagrożenia dla ochrony osób fizycznych, szczególnie w związku z działaniami realizowanymi w Internecie. Okoliczność ta sprzyja również wykonywaniu pracy, w ramach której przetwarzanie danych osobowych odbywa się w przestrzeni wirtualnej. W wielu takich sytuacjach miejsce wykonywania pracy staje się sprawą drugorzędną, bowiem przy zapewnieniu pracownikowi odpowiedniego sprzętu oraz dostępu do Internetu i określonych systemów informatycznych zadania służbowe mogą być realizowane w zasadzie z dowolnej lokalizacji. Wiąże się to jednak z dodatkowymi zagrożeniami dla ochrony danych osobowych. Dostrzegł to ustawodawca już na etapie wprowadzania do Kodeksu pracy instytucji telepracy[1].

Szeroko rozumiana „praca na odległość" funkcjonowała od wielu lat jako telepraca. Zgodnie z definicją ustawową telepracy zawartą w art. 67^5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy[2] praca mogła być wykonywana regularnie poza zakładem pracy z wykorzystaniem środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną. Taki sposób organizowania pracy określany był mianem telepracy, a pracownik, który wykonywał pracę w powyższych warunkach i przekazywał pracodawcy wyniki pracy, w szczególności za pośrednictwem środków komunikacji elektronicznej, określany był jako telepracownik[3].

Telepraca mogła wynikać z postanowień umowy o pracę bądź porozumienia pracodawcy i pracownika. Niezbędna była zgoda pracownika na wykony-

---

[1] M. Kuba, *Ochrona danych osobowych w kontekście pracy zdalnej – wybrane zagadnienia*, [w:] M. Mędrala (red.), *Praca zdalna w polskim systemie prawnym*, 2021, Lex.

[2] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2021 r., poz. 1162 ze zm.), dalej jako k.p.

[3] S. Kryczka, *Praca zdalna pod kontrolą Państwowej Inspekcji Pracy*, 2020, Lex.

wanie tej formy pracy, a jej czas był zależny zarówno od woli pracownika, jak i pracodawcy[4].

Na pracodawcę nałożono bowiem obowiązek ustalenia zasad ochrony danych przekazywanych telepracownikowi oraz przeprowadzania – w miarę potrzeby – instruktażu i szkolenia w tym zakresie (art. 67^{11} § 1 k.p.). Przepisy dotyczące telepracy dawały również możliwość przeprowadzenia kontroli wykonywania przez pracownika telepracy w domu telepracownika, jednak musiała ona być zapowiedziana i odbywać się za jego zgodą. Mimo braku w ustawie covidowej analogicznych regulacji odnoszących się do pracy zdalnej, należy przyjąć, że powyższe kwestie są istotne także w przypadku korzystania przez pracodawcę z pracy zdalnej, w ramach której pracownik uzyskuje dostęp do danych osobowych[5]. Telepracownik potwierdzał na piśmie zapoznanie się z tymi zasadami ochrony danych oraz był zobowiązany do ich przestrzegania[6]. Podkreślenia wymaga tutaj rola doradcza i monitorująca IOD i jego poprzednika – administratora bezpieczeństwa informacji, który odpowiadał za stosowne działania uświadamiające poprzez wskazywanie istotnych ryzyk i zagrożeń związanych z wykonywaniem telepracy i bezpiecznych zasad jej świadczenia oraz polegająca na przeprowadzaniu kontroli w miejscu wykonywania telepracy. Pracodawca mógł telepracownikowi powierzyć sprzęt służbowy do pracy, który musiał ubezpieczyć oraz pokryć koszty związane z instalacją, serwisem, eksploatacją i konserwacją tego sprzętu. Obowiązkiem pracodawcy było również zapewnienie telepracownikowi pomocy technicznej i niezbędnych szkoleń w zakresie obsługi sprzętu. Strony mogły również postanowić w odrębnej umowie, że pracownik będzie pracował na własnym sprzęcie. Wówczas pracodawca musiał mu za to wypłacać ekwiwalent pieniężny. Kodeks wskazywał, że przy jego ustalania pracodawca powinien wziąć pod uwagę normy zużycia sprzętu, jego udokumentowane ceny rynkowe oraz ilość wykorzystywanego materiału na potrzeby pracodawcy[7].

W literaturze przedmiotu zostało wskazane, że wśród zawodów, dla których taka forma zatrudnienia mogła być atrakcyjna, byli m.in. dziennikarze, pisarze, tłumacze, projektanci, architekci, programiści, a także pracownicy firm inwestycyjnych, maklerzy przedstawicieli handlowych, ubezpieczeniowych, księgowych, osoby zajmujące się usługami serwisowymi, tworzeniem i administrowaniem stronami internetowymi, działalnością edytorsko-redakcyjną i komputerowym składem tekstu, działalnością marketingową, przeprowadzaniem badań ankietowych lub telefonicznym rynku[8].

---

[4] A. Nowicki, *Praca zdalna a telepraca – czym się różnią?*, https://kadry.infor.pl/kadry/inne_formy_zatrudnienia/telepraca/4710942,Praca-zdalna-a-telepraca-czym-sie-roznia.html (data dostępu: 6.10.2024).

[5] M. Kuba, op. cit.

[6] M. Mędrala, *Praca zdalna. Komentarz do nowelizacji Kodeksu pracy*, 2023, Lex.

[7] M. Nowicka, *Telepraca – forma elastycznego zatrudnienia*, 2023, Lex.

[8] Ibidem.

Pandemia COVID-19 przyczyniła się do rozwoju i wdrożenia pracy zdalnej zarówno w przedsiębiorstwach prywatnych, jak również w administracji publicznej. Spowodowało to wydanie wytycznych w związku z pracą zdalną przez Urząd Ochrony Danych Osobowych, jak i Europejską Agencję Bezpieczeństwa Sieci i Informacji. Okoliczności te zostały zidentyfikowane jako podwyższające ryzyko naruszenia przepisów[9] 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[10]. Celem jej wprowadzenia było ograniczenie kontaktów i możliwości rozprzestrzeniania się wirusa pomiędzy pracownikami i interesariuszami[11]. Istotnym powodem takiej reakcji ww. instytucji był znaczny wzrost liczby incydentów cyberbezpieczeństwa zgłaszanych przez użytkowników i zarejestrowanych przez CERT Polska (pierwszy powstały w Polsce zespół reagowania na incydenty komputerowe) w stosunku do lat poprzednich od czasu rozpoczęcia pandemii. Warto podkreślić, że liczba zgłaszanych incydentów stale rośnie, począwszy od 29 483 zarejestrowanych incydentów w 2021 r. do 80 267 na koniec roku 2023, podczas, gdy w 2014 r. liczba tego typu incydentów wyniosła 613.

Od marca 2020 r. w celu przeciwdziałania pandemii COVID-19 pracodawca mógł polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna)[12]. Zgodnie z art. 3 ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[13] ustawodawca dopuścił możliwość polecenia pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania w celu przeciwdziałania COVID-19. Powyższy przepis miał zastosowanie w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19 oraz w okresie 3 miesięcy po ich odwołaniu. Jednakże pracodawca mógł w każdym czasie cofnąć polecenie wykonywania pracy zdalnej. Początkowo było to 180 dni od dnia wejścia w życie u.s.r.z.z., tj. do 4 września 2020 r.[14] Dodatkowo praca

[9] Zob. M. Krzyszkowska-Dąbrowska, *Praca zdalna. Praktyczny przewodnik*, Warszawa 2020.

[10] 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.U. UE L 2016.119.1), dalej jako RODO.

[11] M. Mędrala, *Praca zdalna w administracji*, 2023, Lex.

[12] J. Marciniak, *Praca zdalna*, 2020, Lex.

[13] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020 r., poz. 1842 ze zm.), dalej jako u.s.r.z.z.

[14] Zob. J. Marciniak, *Praca zdalna*.

zdalna w administracji publicznej była regulowana rozporządzeniem Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[15]. Zgodnie z kilkukrotnie zmienianym § 22 r.u.o.o. w urzędach administracji publicznej lub jednostkach organizacyjnych wykonujących zadania o charakterze publicznym kierownicy urzędów administracji publicznej, dyrektorzy generalni urzędów lub kierujący jednostką organizacyjną polecali pracownikom wykonywanie pracy zdalnej, z wyjątkiem jednostek organizacyjnych sądów i prokuratury oraz uczelni[16]. Ponadto z dniem 24 czerwca 2020 r. w art. 3 ust. 3 u.s.r.z.z. określono, że wykonywanie pracy zdalnej mogło zostać polecone, jeżeli pracownik miał umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy i pozwalał na to rodzaj pracy. Narzędzia i materiały potrzebne do wykonywania pracy zdalnej oraz obsługę logistyczną pracy zdalnej zapewniał pracodawca. Przepis nie określał sposobu ani kryteriów, na podstawie których pracodawca miałby zweryfikować warunki lokalowe pracownika czy też możliwości techniczne, jakimi ten dysponuje. Można więc przyjąć, że jeżeli pracownik, składając oświadczenie, iż nie ma warunków do pracy zdalnej, ograniczał prawo pracodawcy do wprowadzenia pracy zdalnej. Z uwagi na to, że ustawa nie precyzowała, jakie umiejętności powinien posiadać zatrudniony, aby pracować zdalnie, to do pracodawcy należała ocena, czy dany pracownik posiada odpowiednie cechy, wiedzę i umiejętności, które pozwolą mu efektywnie wykonywać czynności zawodowe w formule zdalnej. Odnośnie do postanowień dotyczących korzystania z narzędzi lub materiałów niezapewnionych przez pracodawcę przy wykonywaniu pracy zdalnej pracownik mógł ich używać pod warunkiem, że umożliwia to poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę[17].

W doktrynie panuje zgodność co do tego, że praca zdalna i telepraca są różnymi formami wykonywania pracy, nie było więc podstaw, aby w kwestiach nieuregulowanych w ustawie stosowano odpowiednio przepisy o telepracy. Do podstawowych różnic należały: czas wykonywania pracy (praca zdalna wykonywana jest okresowo, a telepraca często przez czas nieokreślony, lecz w sposób regularny), sposób wprowadzenia danej formy wykonywania pracy (praca zdalna – na podstawie polecenia pracodawcy; telepraca – na mocy porozumienia stron, w niektórych przypadkach na wniosek pracownika). Zwraca się tak-

---

[15] Rozporządzenie Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz.U. z 2021 r., poz. 861), dalej jako r.u.o.o.

[16] M. Mędrala, *Praca zdalna w administracji…*

[17] J. Marciniak, *Praca zdalna – aspekty prawne*, [w:] J. Marciniak (red.), *Praca zdalna i hybrydowa. Aspekty organizacyjne i prawne*, 2023, Lex.

że uwagę na konsekwencje odmowy wykonywania pracy w formie zdalnej – jeżeli byłaby nieuzasadniona, pracownik mógł podlegać odpowiedzialności porządkowej, a pracodawca miał możliwość rozwiązania umowy o pracę za wypowiedzeniem lub bez wypowiedzenia, natomiast w przypadku telepracy pracownik nie mógł ponosić jakichkolwiek konsekwencji w przypadku braku zgody na tę formę pracy. Warto także zwrócić uwagę, że wyniki pracy zdalnej, inaczej niż w przypadku telepracy, nie musiały być przekazywane za pośrednictwem komunikacji elektronicznej[18].

Mając powyższe na uwadze, dotychczasowe rozwiązania wynikające z przepisów k.p. dotyczące telepracy były dużo bardziej korzystne zarówno dla pracodawcy, jak i dla pracowników, a sposób funkcjonowania pracy na odległość jest rozwiązaniem występującym od wielu lat tak w sektorze prywatnym, jak i publicznym.

Zapowiedzi nowelizacji k.p. stały się faktem i 7 kwietnia 2023 r., po dwumiesięcznym *vacatio legis*, zaczęły obowiązywać przepisy o pracy zdalnej, wprowadzone ustawą z dnia 1 grudnia 2022 r. o zmianie ustawy Kodeks pracy oraz niektórych innych ustaw[19]. Należy podkreślić, że wiele rozwiązań zostało zaczerpniętych w oparciu o rozwiązania wynikające z telepracy. I tak, zgodnie z art. 67^{18} k.p.[20], praca może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (praca zdalna). Podobnie jak w przypadku innych pracodawców (w szczególności sektora prywatnego) w administracji publicznej są możliwe do zastosowania 4 tryby pracy zdalnej:

– model podstawowy – w ramach uzgodnień między pracodawcą a pracownikiem (art. 67^{19} § 1–2 k.p.),

– model nadzwyczajny – w drodze polecenia pracodawcy (art. 67^{19} § 3–5 k.p.),

– model uprzywilejowany – na wniosek niektórych szczególnych grup pracowników (art. 67^{19} § 6–7 k.p.),

– model doraźny – tzw. okazjonalna praca typu *home office* w wymiarze do 24 dni w ciągu roku na wniosek pracownika (art. 67^{33} k.p.).

Zasady wykonywania pracy zdalnej, podobnie jak warunki stosowania telepracy, są bowiem określane w:

– porozumieniu zawieranym między pracodawcą i zakładową organizacją związkową (zakładowymi organizacjami zawodowymi – wszystkimi, a jeżeli

[18] J. Unterschütz, *Pojęcia telepracy i pracy zdalnej. dotychczasowe doświadczenia i regulacje prawne*, [w:] M. Mędrala (red.), op. cit., s. 22.

[19] Ustawa z dnia 1 grudnia 2022 r. o zmianie ustawy Kodeks pracy oraz niektórych innych ustaw (Dz.U. z 2023 r., poz. 240 ze zm.).

[20] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2023 r., poz. 1465).

nie jest możliwe uzgodnienie treści porozumienia ze wszystkimi zakładowymi organizacjami związkowymi – z reprezentatywnymi zakładowymi organizacjami związkowymi w rozumieniu ustawy o związkach zawodowych, z których każda zrzesza co najmniej 5% pracowników zatrudnionych u pracodawcy),

– regulaminie – jeżeli nie dojdzie do zawarcia porozumienia z zakładową organizacją związkową (zakładowymi organizacjami zawodowymi) oraz w przypadku gdy u pracodawcy nie działa żadna zakładowa organizacja związkowa – po konsultacji z przedstawicielami pracowników.

W literaturze akcentuje się, że wykonywanie pracy zdalnej jest dopuszczalne także wtedy, gdy nie zostanie zawarte porozumienie albo nie zostanie wydany regulamin. Wówczas pracodawca określa zasady wykonywania pracy zdalnej odpowiednio w poleceniu wykonywania pracy zdalnej, o którym mowa w art. 67^{19} § 3 k.p., albo w porozumieniu zawartym z pracownikiem (art. 67^{20} § 5 k.p.)[21]. Ustawa określa, co powinno regulować porozumienie lub regulamin. W aktach tych należy ustalić:

– grupy pracowników, które mogą być objęte pracą zdalną,

– zasady pokrywania przez pracodawcę kosztów związanych z wykonywaniem pracy zdalnej,

– zasady ustalania ekwiwalentu pieniężnego lub ryczałtu,

– zasady porozumiewania się pracodawcy i pracownika wykonującego pracę zdalną, w tym sposób potwierdzania obecności pracownika wykonującego pracę zdalną na stanowisku pracy,

– zasady kontroli wykonywania pracy przez pracownika wykonującego pracę zdalną,

– zasady kontroli w zakresie bezpieczeństwa i higieny pracy,

– zasady kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych,

– zasady instalacji, inwentaryzacji, konserwacji, aktualizacji oprogramowania i serwisu powierzonych pracownikowi narzędzi pracy, w tym urządzeń technicznych[22].

W tym miejscu warto przedstawić pogląd wyrażony w literaturze przedmiotu, zgodnie z którym to pracodawca powinien zapewnić pracownikom zdalnym należyty instruktaż dotyczący pracy na danym stanowisku adekwatny do stopnia trudności wykonywanych zadań, podobnie jak pracownikom „stacjonarnym". Do podmiotu zatrudniającego należy wybór środka umożliwiającego realizację tego celu[23]. Przepis nie określa sposobu czy też kryteriów, na podstawie których pracodawca miałby zweryfikować warunki lokalowe pracownika lub możliwości techniczne, jakimi dysponuje. Można więc przy-

[21] M. Mędrala, *Praca zdalna w administracji…*

[22] I. Baranowska, *Nowelizacja kodeksu pracy – praca zdalna i badanie trzeźwości pracowników*, 2021, Lex.

[23] M. Krzyszkowska-Dąbrowska, op. cit.

jąć, że jeżeli pracownik złoży oświadczenie, że nie ma warunków do pracy zdalnej, to prawo pracodawcy do wprowadzenia pracy zdalnej zostanie ograniczone[24].

Ponadto w literaturze przedmiotu zwrócono uwagę, że do podstawowych obowiązków pracownika należy sumienne i staranne wykonywanie pracy oraz stosowanie się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa lub umową o pracę (art. 100 § 1 k.p.). Inne zobowiązania nałożone ustawowo na osobę zatrudnioną dotyczą m.in. przestrzegania czasu pracy ustalonego w zakładzie pracy, przestrzegania regulaminu pracy i ustalonego w zakładzie pracy porządku, przestrzegania przepisów oraz zasad bhp, a także przepisów przeciwpożarowych, dbania o dobro pracodawcy, ochrony jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie narazić mogłoby go na szkodę, przestrzegania tajemnicy określonej w odrębnych przepisach, a także przestrzegania w zakładzie pracy zasad współżycia społecznego. Wszystkie wskazane obowiązki będą aktualizować się podczas pracy zdalnej[25].

Istotnym przepisem z punktu widzenia pracodawcy oraz IOD jest art. 67[26] § 1 k.p., wskazujący, że pracodawca określa procedury ochrony danych osobowych oraz przeprowadza, w miarę potrzeby, instruktaż i szkolenie w tym zakresie. Zgodnie z § 2 wskazanego przepisu pracownik wykonujący pracę zdalną potwierdza w postaci papierowej lub elektronicznej zapoznanie się z procedurami, o których mowa w § 1, oraz jest obowiązany do ich przestrzegania. W komentowanym przepisie mowa jest o „procedurach", co sugeruje konieczność wprowadzenia odrębnych dodatkowych dokumentów w tym zakresie. Mogą być one oczywiście wyodrębnioną częścią ogólnej polityki bezpieczeństwa u pracodawcy. Z kolei przeprowadzenie instruktażu i szkolenia nie jest obowiązkowe. Pracodawca powinien samodzielnie ocenić konieczność jego przeprowadzenia, co w kontekście ciągle rosnącej liczby zgłaszanych incydentów wydaje się bezdyskusyjne. Jeśli u danego pracodawcy został wyznaczony IOD, to pracodawca powinien skorzystać z jego doradztwa, podobnie jak to miało miejsce w przypadku telepracy. W ramach szkolenia z zakresu procedur ochrony danych osobowych szczególnie istotne pozostaje zapoznanie pracowników z zasadami ochrony danych osobowych zarówno w obszarze techniczno-organizacyjnym, jak i związanych z procedurami dotyczącymi obsługi naruszeń ochrony danych osobowych czy reagowania na żądania osób, których dane dotyczą[26]. Pracownik wykonujący pracę zdalną będzie musiał potwierdzić, w postaci papierowej lub elektronicznej, zapoznanie się z ww. procedurami oraz ich przestrzegać.

---

[24] J. Marciniak, *Praca zdalna.*

[25] M. Krzyszkowska-Dąbrowska, op. cit.

[26] M. Mędrala, *Praca zdalna. Komentarz do nowelizacji…*

Warto w tym miejscu wskazać, że pracodawca może przeprowadzać kontrolę wykonywania pracy przez pracownika zdalnego, w tym w zakresie bezpieczeństwa i higieny pracy. Zasady tej kontroli muszą być określone odpowiednio w porozumieniu z zakładową organizacją związkową, regulaminie, poleceniu pracodawcy lub porozumieniu z pracownikiem. Pracodawca będzie obowiązany dostosować sposób przeprowadzania kontroli do miejsca wykonywania i charakteru pracy zdalnej. Jeżeli pracodawca w trakcie kontroli pracy zdalnej uzgodnionej w trakcie zatrudnienia stwierdzi uchybienia w przestrzeganiu przepisów i zasad w zakresie bezpieczeństwa i higieny pracy określonych w informacji zawierającej zasady i sposoby właściwej organizacji stanowiska pracy (przygotowanej wcześniej na podstawie wyników oceny ryzyka zawodowego), wezwie pracownika do usunięcia stwierdzonych uchybień we wskazanym terminie albo cofnie zgodę na wykonywanie pracy zdalnej przez tego pracownika. W przypadku wycofania zgody na wykonywanie pracy zdalnej pracownik rozpoczyna pracę w miejscu i terminie określonym przez pracodawcę[27]. Z kolei kontrola w zakresie bezpieczeństwa informacji i ochrony danych osobowych, w tym procedur ochrony danych osobowych, powinna dotyczyć sposobu przestrzegania przez pracownika obowiązujących zasad ochrony danych osobowych przyjętych u pracodawcy, potwierdzenia uczestnictwa pracownika w szkoleniach z zakresu ochrony danych osobowych oraz weryfikacji narzędzi i systemów, za pośrednictwem których pracownik uzyskuje dostęp do danych osobowych pracodawcy. Pracodawca określa w regulaminie, kiedy dokonuje kontroli w czasie pracy.

Kolejne postanowienia dotyczą wyposażenia stanowiska pracy (np. pracodawca dostarcza niezbędny sprzęt wraz z oprogramowaniem do wykonywania pracy zdalnej). Ten dostarczony sprzęt ma odpowiadać normom bezpieczeństwa i posiadać stosowne certyfikaty, a na pracodawcy spoczywa obowiązek ubezpieczenia sprzętu oraz pokrywania kosztów związanych z instalacją, serwisem i konserwacją sprzętu. Ponadto pracodawca jest obowiązany zapewnić pracownikowi pomoc techniczną i niezbędne szkolenie w zakresie obsługi sprzętu. W regulaminie powinny znaleźć się zasady korzystania ze sprzętu należącego do pracownika, uwzględniając w szczególności odpowiedzialności pracownika, który zwykle jest obowiązany w szczególności:

– dbać o dostarczony sprzęt pracodawcy,

– nie korzystać ze sprzętu w sposób niezgodny z przepisami prawa (np. zamieszczać nielegalne oprogramowanie),

– nie używać dodatkowych programów bez zgody pracodawcy,

– nie udostępniać sprzętu członkom rodziny lub innym osobom,

– w przypadku uszkodzenia (awarii) sprzętu, powstania zagrożenia dla zdrowia lub życia pracownika jest on obowiązany powstrzymać się od wykonywania pracy i zawiadomić o tym niezwłocznie pracodawcę,

[27] I. Baranowska, op. cit.

– pracownik ponosi odpowiedzialność materialną za powierzony sprzęt, z obowiązkiem zwrotu lub do wyliczenia się, sprzęt lub inne mienie, na zasadach przewidzianych w k.p.[28]

Nawiązując do wspomnianych wcześniej zasad kontroli wykonywania pracy zdalnej, o których mowa w porozumieniu lub regulaminie, należy mieć na uwadze art. 67^{28} k.p. W świetle § 1 wskazanego przepisu pracodawca ma prawo przeprowadzać kontrolę wykonywania pracy zdalnej przez pracownika, kontrolę w zakresie bezpieczeństwa i higieny pracy lub kontrolę przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, na zasadach określonych w porozumieniu czy w regulaminie. Kontrolę przeprowadza się w porozumieniu z pracownikiem w miejscu wykonywania pracy zdalnej w godzinach pracy pracownika, analogicznie jak w przypadku telepracy. Na podstawie § 2 ww. przepisu pracodawca dostosowuje sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju. Wykonywanie czynności kontrolnych nie może naruszać prywatności pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem. Jeżeli pracodawca w trakcie kontroli pracy zdalnej, o której mowa w art. 67^{19} § 1 pkt 2, stwierdzi uchybienia w przestrzeganiu przepisów i zasad w zakresie bezpieczeństwa i higieny pracy określonych w informacji, o której mowa w art. 67^{31} § 5, lub w przestrzeganiu wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych, zobowiązuje pracownika do usunięcia stwierdzonych uchybień we wskazanym terminie albo cofa zgodę na wykonywanie pracy zdalnej przez tego pracownika. W przypadku wycofania zgody na wykonywanie pracy zdalnej pracownik rozpoczyna pracę w dotychczasowym miejscu pracy w terminie określonym przez pracodawcę.

Ochrona danych osobowych w związku z funkcjonowaniem pracy na odległość i rola IOD w przedmiotowym zakresie

Wprowadzenie przepisów RODO przyniosło wyzwania dla administratorów danych osobowych (także tych będących pracodawcami), związane zwłaszcza z koniecznością dostosowania procesów przetwarzania danych osobowych do wprowadzonych wymagań. Ich respektowanie jest o tyle istotne, że prawodawca unijny wprowadził system administracyjnych kar pieniężnych z tytułu określonych w art. 83 ust. 4–5 RODO naruszeńp[29]. Na gruncie wskazanych przepisów o ochronie danych osobowych pracodawca występuje w roli admini-

[28] M. Marciniak, *Praca zdalna – aspekty...*
[29] M. Kuba, op. cit.

stratora danych osobowych (art. 4 pkt 7 RODO). Możliwe jest także korzystanie przez niego z podmiotów przetwarzających (art. 4 pkt 8 RODO), np. podmiotów dostarczających określonego oprogramowania wykorzystywanego w trakcie pracy zdalnej. Zarówno pracodawca, jak i pracownik zdalny związani są ogólnymi regułami ochrony danych osobowych na gruncie RODO. Zdalne świadczenie pracy z założenia implikuje zwiększone problemy w zakresie przetwarzania danych osobowych. Związane jest to z korzystaniem z wielu zdalnych narzędzi pracy oraz dodatkowym ryzykiem związanym z bezpieczeństwem danych osobowych w trakcie pracy w domu[30]. Rozpoczynając rozważania dotyczące przepisów prawnych regulujących funkcjonowanie pracy zdalnej, należy wskazać, że przepisy RODO nie regulują, jak ma być wykonywana praca zdalna. Nie możemy jednak zapomnieć, że podczas wykonywania pracy zdanej dochodzi do przetwarzania danych osobowych. Istotnym przepisem jest art. 5 RODO, który określa zasady dotyczące przetwarzania danych osobowych, tj. wskazuje, że dane osobowe muszą być:

– przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,

– zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

– adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

– prawidłowe i w razie potrzeby uaktualniane,

– 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,

– 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.

Podkreślenia wymagają zasady integralności i poufności oraz rozliczalności. Pierwsza z nich wynika z art. 5 ust. 1 lit. f RODO i stwierdza, że przetwarzanie danych powinno odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, a administrator powinien zagwarantować ich ochronę przed niedozwolonym lub niezgodnym z prawem użyciem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Z kolei zasada rozliczalności określona w art. 5 ust. 2 RODO precyzuje, że administrator powinien być w stanie wykazać, że przestrzegane są podstawowe zasady RODO, o których mowa powyżej, a zatem dysponować stosownym dowodem potwierdzającym, że przyjęte środki są adekwatne i zostały odpowiednio wdrożone, a pracownicy przeszkoleni w tym zakresie i świadomi występujących ryzyk i zagrożeń oraz

[30] M. Mędrala, *Praca zdalna. Komentarz do nowelizacji…*

działań zaradczych. Zgodnie z art. 32 RODO administrator danych ma obowiązek wdrożyć odpowiednie środki organizacyjne i techniczne w celu zapewnienia odpowiedniego bezpieczeństwa. Obowiązuje to również podczas wykonywania pracy zdalnej – tutaj pracodawca ma utrudnione zadanie, ponieważ nie zna warunków, w jakich praca jest wykonywana[31]. Dla uznania, czy zastosowane instrumenty ochrony danych są odpowiednie, administrator i podmiot przetwarzający powinien samodzielnie to ustalić, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych, a w zakresie bezpieczeństwa przetwarzania również stan wiedzy technicznej, koszt wdrażania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Na powyższe wskazuje również Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z 26 sierpnia 2020 r.[32], stwierdził, że art. 32 RODO „(...) nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością". Sąd podkreślił również, że „przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka". Nie sposób nie wskazać również obowiązków wynikających z przepisów art. 24, 29 i 32 RODO w zakresie nadawania przez administratora upoważnień osobom mającym dostęp do danych osobowych. Pracodawcy jako administratorzy danych mają obowiązek zapewnić przestrzeganie zasad przetwarzania danych, w tym zagwarantować ich bezpieczeństwo, a pracownicy stosować się do przyjętych zasad i procedur w tym zakresie, co nie znaczy, że pracodawca może przerzucić odpowiedzialność na pracownika, w sytuacji gdy przekazany mu do pracy zdalnej sprzęt nie został odpowiednio skonfigurowany i zabezpieczony, np. poprzez szyfrowanie.

Przy określaniu sposobów przetwarzania administrator został zobligowany, aby uwzględnić ochronę danych i prywatności na każdym etapie tworzenia oraz funkcjonowania mechanizmów i technologii obejmujących ich przetwarzanie. Warto przy tym zwrócić uwagę na sformułowanie „przy określaniu sposobów przetwarzania", użyte w art. 25 ust. 1 RODO. Administrator danych

---

[31] Ł. Prasolek, A. Kiełbratowska, *Praca zdalna w praktyce. Zagadnienia prawa pracy i RODO*, [w:] Ł. Prasołek (red.), *Pomoc dla pracodawcy w sprawach pracowniczych w dobie kryzysu. Tarcza antykryzysowa, prawo pracy, RODO, ZUS, PIT*, Warszawa 2020, s. 17–18.

[32] Wyrok WSA w Warszawie z 26 sierpnia 2020 r., sygn. akt II SA/Wa 2826/19, Lex nr 3067899.

został tym określeniem zobowiązany do planowania *ex ante* i stosowania instrumentów zapewniających zgodność z RODO już na etapie prac związanych z przygotowaniem działań, w ramach których zamierza przetwarzać dane. Zasada prywatności w fazie projektowania, tzw. *privacy by design*, określona w art. 25 ust. 1 RODO, zobowiązała administratora do uwzględniania ochrony danych osobowych już podczas planowania instrumentów, mechanizmów, urządzeń, systemów, aplikacji i procesów, które miałyby w przyszłości zostać użyte do przetwarzania danych. Administrator powinien w każdym takim przypadku podjąć działania przygotowawcze, testy i badania, zorientowane na zapewnienie możliwie najwyższego poziomu bezpieczeństwa przetwarzanym danym[33]. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, zwłaszcza 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[34].

Zarówno w trakcie wykonywania pracy zdalnej, jak i podczas pracy w biurze może dochodzić do naruszeń ochrony danych osobowych. Zgodnie z definicja z art. 4 pkt 12 RODO naruszenie danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Żeby doszło do naruszenia muszą być spełnione łącznie trzy przesłanki:

– naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,

– skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,

– naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

Grupa Robocza Art. 29[35] w wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01) wyróżnia trzy typy naruszeń ochrony danych osobowych:

– „naruszenie dotyczące poufności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych,

---

[33] S. Hady-Głowiak, D. Kozłowski, *Dekalog ochrony danych osobowych – stosowanie zasad przetwarzania danych osobowych jako podstawa bezpieczeństwa przetwarzania danych*, [w:] J. Wołejszo, K. Rejman, M. Wilczyńska (red.), *Bezpieczeństwo informacji w organizacjach*, Kalisz 2021, s. 12–13.

[34] M. Mędrala, *Praca zdalna. Komentarz do nowelizacji*….

[35] Grupa ta została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Jej zadania zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

– „naruszenie dotyczące integralności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych,

– „naruszenie dotyczące dostępności danych" – naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych[36].

Praktyka pokazuje, że wielu administratorów wcześniej – jeszcze przed pandemią koronawirusa – przewidywało wykonywanie pracy poza siedzibą pracodawcy w związku z telepracą bądź też w związku z regulowaniem zagadnień dotyczących z pracy z wykorzystaniem urządzeń mobilnych[37]. Taka praktyka funkcjonowała w szczególności w sektorze prywatnym. Z kolei w sektorze publicznym w związku z pandemią wiele urzędów nie posiadało rozwiązań zarówno technicznych, jak i organizacyjnych do rozpoczęcia pracy w formie zdalnej, co nie oznacza, że nie było dobrych praktyk w wielu instytucjach w tym zakresie, gdzie istniały rozwiązania przyjęte w oparciu o procedury i mechanizmy funkcjonujące w związku ze świadczeniem przez pracowników telepracy.

Brak wdrożenia odpowiednich rozwiązań technicznych, jak i organizacyjnych otwierał drogę do ataków, tym bardziej że większość urzędników nie otrzymała służbowego sprzętu, nie przeszła odpowiednich szkoleń z zakresu bezpieczeństwa IT, nie aktualizuje na bieżąco oprogramowania, a zarządzający urzędami nie dokonują gradacji uprawnień dostępu m.in. do serwera gminy[38]. O ile jednak w pierwszej fazie pandemii praca zdalna w administracji publicznej była stosowana na szeroką skalę, o tyle później stopniowo jej znaczenie malało. Z kolei w sektorze prywatnym praca z wykorzystaniem urządzeń mobilnych stosowana w szczególności w dużych korporacjach międzynarodowych jest dosyć powszechnym rozwiązaniem z uwagi na wieloletnie rozwiązania i doświadczenia w tym obszarze. W administracji wskazywano przede wszystkim na mniejszą efektywność tej pracy w zakresie załatwiania spraw obywateli. Obserwacje te potwierdzają kontrole przeprowadzone przez Najwyższą Izbę Kontroli (dalej jako NIK). W 2020 r. w 10 kontrolowanych przez NIK urzędach z inicjatywy pracodawcy zdalnie pracowało niemal 73% zatrudnionych tam osób, na własną prośbę – 9,5%, natomiast w 2021 r. 47,5% zatrudnionych pracowało zdalnie na polecenie pracodawcy, a na swój wniosek – 12,5%[39].

W 40 podmiotach objętych kontrolą wprowadzono, opracowano i wdrożono właściwe procedury wewnętrze i z reguły prawidłowo ewidencjonowano czas

---

[36] Ł. Prasolek, A. Kiełbratowska, op. cit., s. 20.

[37] M. Sakowska-Baryła, *Ochrona danych osobowych w warunkach pracy zdalnej*, Warszawa 2020, s. 35.

[38] R. Horbaczewski, *Gdy urzędnik pracuje w domu, hakerowi łatwiej wejść do urzędu*, 2022, Lex.

[39] M. Mędrala, *Praca zdalna w administracji…*

pracy zdalnej, jednak bariery infrastrukturalne, finansowe i techniczne ograniczyły lub uniemożliwiły odpowiednie zorganizowanie efektywnej pracy zdalnej. Większość (29 z 40) skontrolowanych podmiotów wyposażona była bowiem w niewielką liczbę przenośnego sprzętu komputerowego, niemal połowa nie miała zdigitalizowanych danych, a w 17 nie można było użytkować systemów dziedzinowych poza siedzibą jednostki, co uniemożliwiało zdalny dostęp do dokumentów. Ponad rok doświadczeń z pracą zdalną pozwolił kierownikom skontrolowanych jednostek na zdiagnozowanie korzyści i barier w organizowaniu tego typu pracy. Korzyści identyfikowano najczęściej w podmiotach, które były stosunkowo najlepiej przygotowane do takiego trybu pracy. Były to m.in. zwiększenie bezpieczeństwa pracowników czy oszczędności w zakresie kosztów i czasu dojazdów do pracy. Znacznie częściej wskazywano jednak na bariery, zwracając głównie uwagę na specyfikę realizowanych zadań oraz brak odpowiedniego wyposażenia podmiotów publicznych w sprzęt komputerowy i rozwiązania techniczne zapewniające zdalny dostęp do dokumentów[40].

Mając powyższe na uwadze i wiele korzyści w związku ze świadczeniem pracy w formie zdalnej i telepracy, głównym ryzykiem związanym z wykonywaniem pracy na odległość był brak wdrożenia w instytucji odpowiednich zasad i procedur lub ich niezgodność z przepisami powszechnie obowiązującego prawa, w tym brak odpowiedniej świadomości kierownictwa oraz pracowników w tym zakresie. Kolejnym problemem był brak stosownych rozwiązań technicznych i organizacyjnych oraz brak funkcjonowania zasad zapewnienia ciągłości działania, w szczególności w sektorze publicznym. Powyższe mogło powodować zagrożenia związane z możliwością wycieku danych, utraty posiadanych zasobów oraz dostępu do danych osób nieuprawnionych.

Właściwe dokumentowanie pracy zdalnej pozwala pracodawcy – odpowiedniemu administratorowi (dalej jako ADO) lub podmiotowi przetwarzającemu na gruncie przepisów RODO – osiągnąć takie cele, jak w szczególności zgodność z przepisami prawa, ustalenie zasad wykonywania pracy zdalnej przez pracowników oraz zapewnienie organizacji pracy zespołu podczas pracy zdalnej i rozliczalności na gruncie RODO. Należy podkreślić ustalenie spójnych reguł bezpieczeństwa, zapewnienia przez pracodawcę wsparcia dla personelu pracującego zdalnie, przeciwdziałania odpowiedzialności prawnej, ewolucji procesów organizacyjnych czy racjonalizacji i dokumentowaniu wydatków[41].

Z wyników kolejnej kontroli NIK, którą objęto kancelarię premiera i 10 instytucji w województwie warmińsko-mazurskim, niewłaściwie zarządzano bezpieczeństwem informacji, ponieważ w połowie skontrolowanych podmiotów nie opracowano i nie wdrożono wymaganego przepisami rozporządze-

[40] Informacja o wynikach kontroli: Delegatura Najwyższej Izby Kontroli w Białymstoku, *Organizacja pracy zdalnej w wybranych podmiotach wykonujących zadania publiczne w związku z ogłoszeniem stanu epidemii*, Warszawa 2021, s. 8.

[41] M. Sakowska-Baryła, op. cit., s. 36.

nia Krajowych Ram Interoperacyjności systemu zarządzania bezpieczeństwem informacji, w którym należało określić sposób postępowania ze wszystkimi kategoriami przetwarzanych informacji. W jednostkach tych ograniczono się do ustalenia zasad dotyczących bezpieczeństwa danych osobowych. W części urzędów nie dokonywano przeglądów regulacji dotyczących zarządzania bezpieczeństwem informacji oraz nie dokonywano ich aktualizacji. W ograniczonym zakresie wykorzystywano zewnętrzny audyt bezpieczeństwa systemów informatycznych. W jednym z urzędów, w których regulacje wewnętrzne umożliwiały wykorzystywanie w pracy zdalnej prywatnych komputerów, nie określono w tym zakresie szczegółowych wymagań dotyczących zasad zapewnienia pożądanego poziomu ochrony informacji. Część jednostek nie stosowała także ustalonych własnych zasad i regulacji, obniżając skuteczność przyjętych rozwiązań w obszarze bezpieczeństwa informacji. Stwierdzone nieprawidłowości dotyczyły m.in. nieprzestrzegania wymogu pracy na indywidualnych kontach systemu operacyjnego, braku szyfrowania dysków twardych komputerów wykorzystywanych w pracy zdalnej, a także nieprzestrzegania przyjętych zasad postępowania z zewnętrznymi nośnikami danych[42].

Okres pandemii przyczynił się w wielu instytucjach do podniesienia świadomości w zakresie bezpieczeństwa informacji i aktualizacji obowiązujących zasad i procedur dotyczących zarówno zasad funkcjonowania pracy na odległość, ale również zgłaszania incydentów i naruszeń, a także zapewnienia ciągłości działania jednostki. Istotą jest tu przede wszystkim okresowy audyt w zakresie bezpieczeństwa informacji, który powinien wskazywać zagrożenia i ryzyka oraz zalecenia dla kierownika jednostki. Obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji w jednostkach sektora finansów publicznych wynika wprost z przepisów prawa[43].

Warto wskazać, że zakres zadań, o których mowa powyżej, oraz rola IOD w organizacji powodują, że każdorazowo w przypadku zmian mogących wpływać na warunki, zasady, sposób, narzędzia i procesy przetwarzania danych osobowych. Inspektor powinien podejmować działania, o których mowa w art. 39 RODO. Jednocześnie, co w świetle art. 5 ust. 2 oraz art. 39 ust. 2 RODO zasługuje na rekomendację, powinien starannie dokumentować podejmowane czynności, aby móc wykazać zgodność działań administratora z RODO oraz wykonywanie swoich zadań z należytą starannością i uwzględnieniem ryzyka[44].

Jedną z kluczowych regulacji zawiera art. 38 RODO, który stanowi, że administrator oraz podmiot przetwarzający zapewniają, „by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy doty-

[42] Informacja o wynikach kontroli: Delegatura Najwyższej Izby Kontroli w Olsztynie, *Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych*, Warszawa 2022, s. 7.

[43] M. Janik, S. Hady-Głowiak, *Bezpieczeństwo informacji jako zadanie jednostek sektora finansów publicznych*, „Studia Prawnoustrojowe" 2023, nr 62, s. 300.

[44] M. Sakowska-Baryła, op. cit., s. 40.

czące ochrony danych osobowych", co wiąże się bezpośrednio ze sprawną i zgodną z prawem realizacją zadań przez IOD.

Zatem przetwarzanie danych osobowych w warunkach pracy zdalnej powinno stać się także przedmiotem działań i analiz IOD, mając na uwadze zmiany organizacji pracy mogące wpływać na warunki, zasady, sposób, narzędzia i procesy przetwarzania danych osobowych oraz związane z tym ryzyka. IOD powinien dokonać analizy obowiązujących w tym zakresie polityk i procedur wewnętrznych oraz udzielić niezbędnych wskazówek i wytycznych w celu dostosowania ich do obowiązujących przepisów dotyczących planowania, wykonywania i raportowania pracy zdalnej, a także w zakresie zapewnienia warunków wykonywania przez pracowników pracy zdalnej i zapewnienia bezpieczeństwa jej świadczenia adekwatnie do zagrożeń. Niezwykle istotne jest również monitorowanie zapoznania się pracowników z warunkami i zasadami wykonywania pracy zdalnej oraz z istniejącymi zagrożeniami w tym zakresie. Tutaj należy mieć na uwadze przede wszystkim wyniki analizy ryzyka związane z wykonywaniem pracy zdalnej, jak również aktualne zagrożenia w obszarze cyberbezpieczeństwa, których liczba stale rośnie.

W kontekście ochrony danych osobowych warto zwrócić uwagę na konieczność realizacji zasad integralności i poufności oraz rozliczalności przetwarzania określonych w art. 5 RODO, które z kolei znajdują odzwierciedlenie zarówno w przepisach określających przesłanki dopuszczalności przetwarzania danych osobowych, a więc w art. 6 i 9 RODO, jak i w wymogach dotyczących bezpieczeństwa danych osobowych, uwzględniania ryzyka naruszeń praw lub wolności osób fizycznych, konieczności dokumentowania przetwarzania danych osobowych w odpowiednich politykach, rejestrach, umowach, dokumentacji związanej z naruszeniami. Kolejnym aspektem jest zabezpieczenie przed odpowiedzialnością administracyjną (uprawnienia naprawcze, w tym administracyjne kary pieniężne orzekane przez organ nadzorczy – Prezesa UODO) przed odpowiedzialnością względem osób, których dane dotyczą, oraz przed sporami prawno-pracowniczymi lub roszczeniami pracowników. Należy również zwrócić uwagę na bezpieczeństwo finansowe pracodawcy. Dokumentowanie pracy zdalnej i posługiwanie się przez pracodawcę stosownymi procedurami przekłada się również na respektowanie interesów pracowników i innych osób w następującym zakresie: poszanowanie dóbr osobistych pracownika, zapewnienie narzędzi, procedur i wsparcia pracowników wykonujących pracę zdalną, udzielanie wsparcia logistycznego, przeciwdziałanie nieprawidłowym działaniom w sieci, przeciwdziałanie odpowiedzialności pracowników. Dotyczy to również zapewnienia adekwatnego standardu przetwarzania danych osobowych bez względu na to, w jaki sposób, gdzie i za pomocą jakich narzędzi są przetwarzane, a także realizacji praw osób, których dane dotyczą, oraz innych praw i wolności osób fizycznych[45].

[45] Ibidem, s. 33–35.

W regulaminach wewnętrznych dotyczących pracy zdalnej, opracowywanych dla pracowników pojawia się warunek, że sprzęt służbowy nie może być wykorzystywany do celów prywatnych. Z wymogów RODO wynika bowiem, że pracodawcy powinni stworzyć regulacje lub uaktualnić już obowiązujące w firmie regulaminy w przedmiotowym zakresie. Jest to jedna z zasad minimalizujących ryzyko naruszenia poufności, np. poprzez zainstalowanie złośliwego oprogramowania lub przypadkowe usunięcie danych przez domownika, który współdzieli z pracownikiem komputer. Powyższe potwierdza również orzecznictwo Sądu Najwyższego z 22 marca 2016 r.[46], z którego wynika, że wyrządzenie pracodawcy szkody przez samowolne używanie telefonu służbowego dla celów lub potrzeb prywatnych nie wyłącza odpowiedzialności odszkodowawczej pracownika na podstawie art. 117 § 2 k.p. Pracownik odpowiada w pełnej wysokości za szkodę, którą wyrządził pracodawcy, korzystając ze sprzętu służbowego do celów prywatnych (np. prowadząc prywatne rozmowy ze służbowego telefonu). Pracownik mógłby się uwolnić od odpowiedzialności, gdyby wykazał, że szkoda powstała w związku z używaniem sprzętu (np. telefonu) w celach służbowych[47]. Już w pierwszych dniach przestawiania się zakładów pracy na pracę zdalną, okazało się, że wyzwaniem jest zapewnienie pracownikom odpowiednich narzędzi do ich realizowania. Wiele instytucji w ogóle nie było na to przygotowanych, w efekcie wymagając od pracowników, aby w domu korzystali ze swojego prywatnego komputera. Brak służbowego laptopa oznaczał brak służbowego sprzętu. Tymczasem bardzo szybko pojawiły się głosy, że przecież w sytuacji, gdy pracownik musi pracować w domu, a do tej pory pracował na urządzeniu stacjonarnym i nie ma możliwości zapewnienia mu laptopa, można wydać mu do domu komputer stacjonarny. Należy zgodzić się ze stanowiskiem Sylwii Czub-Kiełczewskiej, że wydanie pracownikowi choćby sprzętu stacjonarnego przez pracodawcę jest o wiele lepsze, niż zmuszanie pracownika do pracy w domu na prywatnym komputerze. Jeżeli pracodawca nie zapewnił pracownikom służbowego sprzętu, może okazać się, że nie są oni w stanie skutecznie realizować swoich działań, ponieważ muszą udostępnić komputer dzieciom. Nie należy z kolei zgodzić się z twierdzeniem przywołanej autorki, że warto zweryfikować z działami kadr, HR oraz IT kwestię, ilu pracowników pracujących na prywatnym sprzęcie ma dzieci w wieku szkolnym, bowiem powyższe informacje nie mają wpływu na konieczność zapewnienia sprzętu pracownikowi. Jednocześnie dane dotyczące dzieci pracowników są zbierane w konkretnym celu przewidzianym w przepisach prawa pracy (tj. zgłaszania członków rodziny do ubezpieczenia zdrowotnego czy korzystanie z zakładowego funduszu świadczeń socjalnych), a nie

[46] Wyrok SN z 22 marca 2016 r., sygn. akt II PK 31/15, OSNP 2017, Nr 10, poz. 127.

[47] K. Gruca, *Sprzęt służbowy używany przez pracownika do celów prywatnych*, https://poradnikprzedsiebiorcy.pl/-sprzet-sluzbowy-uzywany-przez-pracownika-do-celow-prywatnych (data dostępu: 14.09.2024).

do weryfikacji i zasad przydzielania sprzętu podległym pracownikom. Takie przekazanie powinno odbyć się za pokwitowaniem w formie pisemnej lub elektronicznej (np. podpisanego przez pracownika skanu protokołu przekazania sprzętu)[48].

Mając powyższe na uwadze, IOD powinien dokonać weryfikacji, czy umowy o odpowiedzialności materialnej za powierzone mienie zawierają wymagane postanowienia dotyczące zasad bezpiecznego użytkowania sprzętu (bez względu na rodzaj sprzętu, tj. laptop, modem, router, karta SIM), a także odpowiedzialności za sprzęt i dane na nim zawarte zgodnie ze wzorem wynikającym z obowiązującej w jednostce polityki bezpieczeństwa informacji. Zasady bezpiecznego użytkowania sprzętu czy odpowiedzialności za sprzęt i dane na nim zawarte mogą również wynikać z regulaminu wynoszenia sprzętu lub innej analogicznej procedury. Istotą jest zapoznanie się pracownika z jej postanowieniami, przestrzeganie ich oraz z zasadą odpowiedzialności w tym zakresie. Umowy powierzenia mienia powinny być zawierane na bieżąco z pracownikami jednostki, bez względu na rodzaj sprzętu powierzanego pracownikowi, co zapewnia realizację rozliczalności wynikającej z RODO, bieżącą inwentaryzację mienia firmy/instytucji, a także realizację przez pracodawcę wymogu ustawowego dotyczącego dostarczenia pracownikowi narzędzi i materiałów potrzebnych do wykonywania pracy zdalnej.

W przypadku realizacji przez pracownika zadań przy użyciu sprzętu prywatnego obowiązkiem pracodawcy jako ADO jest zapewnienie odpowiednich środków technicznych i organizacyjnych dla ochrony danych. Wynika to wprost z przepisów art. 24 i 32 RODO i nie można tego obowiązku przerzucić na osoby przetwarzające dane z upoważnienia administratora. Jeżeli pracodawca nie jest w stanie zapewnić pracownikom służbowego sprzętu, troszcząc się o ciągłość własnego biznesu, powinien zapewnić przynajmniej odpowiednie środki ochrony prywatnego sprzętu. Należy przy tym zgodzić się ze stanowiskiem S. Czub-Kiełczewskiej, która uważa, że należy dopuścić możliwość realizowania pracy zdalnej z wykorzystaniem prywatnych komputerów, jednakże przy wsparciu działów informatyki. To bardzo ważne, aby nie ignorować problemów i zapewnić odpowiednie wsparcie. Korzystanie z ogólnodostępnych sieci wi-fi lub współdzielenie Internetu z domownikami w ramach sieci domowej stanowi zagrożenie dla bezpieczeństwa przetwarzanych informacji. Problem ten można rozwiązać, przekazując pracownikom modemy/routery wraz z kartami SIM umożliwiającymi korzystanie z Internetu, ale także uświadamiając pracowników, że większość ich telefonów także daje możliwość udostępnienia Internetu w ramach funkcji *hotspot*. Jest to jedno z najtańszych i najprostszych rozwiązań zwiększających bezpieczeństwo pracy zdalnej. Inspektor ochrony danych we współpracy z informatykiem może opracować prostą instrukcję, jak

[48] S. Czub-Kiełczewska, *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej*, 2020, Lex.

uruchomić funkcję *hotspot* w telefonie i korzystać z tak udostępnionego Internetu na komputerze wykorzystywanym do pracy zdalnej. Pracodawca może, w miarę zapotrzebowania, zwiększyć pakiety przesyłu danych dla poszczególnych kart SIM. To rozwiązanie odciąży także domowe sieci internetowe, które powinny również posiadać hasło do routera, co zwiększy efektywność pracy pracownika[49]. Przenoszenie firmowych danych na prywatne komputery i urządzenia mobilne powinno być zabronione. Dyski, karty pamięci oraz pozostałe elektroniczne nośniki danych muszą zostać zaszyfrowane. Pracownicy powinni posługiwać się silnymi hasłami oraz używać wielopoziomowego uwierzytelniania, co pozwoli ograniczyć dostęp do urządzenia oraz ryzyko utraty danych w przypadku jego zgubienia lub kradzieży. Należy używać wyłącznie zaufanego dostępu do sieci lub chmury i unikać otwartych sieci publicznych[50]. Niezwykle istotnym elementem w przyjętym modelu BYOD (z ang. *Bring Your Own Device* – wykorzystanie sprzętu pracownika w środowisku pracy i w celach służbowych) jest zabezpieczenie narzędzia przed atakami czy też stosowanie zabezpieczeń organizacyjnych poprzez wymuszenie łączenia się z infrastrukturą pracodawcy przez bezpieczne łącze (VPN).

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) zaleciła wprowadzenie określonych zasad oraz wydała przewodnik zawierający podstawowe wskazówki mogące zmniejszyć ryzyka (*cyber hygiene tips*) dla pracodawców i pracowników. Dodatkowo w jej wytycznych szczególny nacisk został położony na ustalenie zakazu instalowania przez pracowników aplikacji i oprogramowań na urządzeniach służbowych, nakazu korzystania przez nich z określonych programów antywirusowych, ostrzeżenia pracujących zdalnie przed możliwością ataków hakerskich i tzw. phishingiem czy przekazywaniem poufnych danych, a także określenie obowiązku zabezpieczenia silnym hasłem prywatnych sieci internetowych używanych w celach służbowych, szyfrowanie przesyłanych wiadomości poczty elektronicznej, oraz zakaz korzystania z prywatnych skrzynek dla celów służbowych lub przesyłania tam materiałów. Zalecane jest także korzystanie z VPN. Znaczenie mogą mieć również takie działania, jak odpowiednia weryfikacja tożsamości uczestników telekonferencji czy wideokonferencji. Szczególnie ostrożnie powinno się, zgodnie z przedmiotowymi wskazówkami, zabezpieczać zewnętrzne nośniki danych. Przeprowadzanie szkoleń i utrzymywanie właściwych zasobów technicznych jest również rekomendowane[51].

Kolejnym ryzykiem, które wiąże się z utratą danych lub dostępem do nich osób nieupoważnionych, jest konieczność wykonywania pracy zdalnej z wykorzystaniem dokumentów papierowych zabranych z biura pracodawcy. Są za-

[49] Ibidem.

[50] E. Jagiełło-Jaroszewska, *Ochrona danych osobowych a telepraca i praca zdalna*, [w:] D. Dörre-Kolasa (red.), *Ochrona danych osobowych w zatrudnieniu*, Warszawa 2020, s. 224.

[51] M. Krzyszkowska-Dąbrowska, op. cit.

wody i specjalizacje, których praca w dużej mierze opiera się na analizie dokumentów i bez nich nie ma możliwości świadczenia pracy z domu. Wielu administratorów danych wprowadziło bezwzględny zakaz wynoszenia przez pracowników jakichkolwiek dokumentów poza siedzibę pracodawcy[52], co należy ocenić pozytywnie[53]. Prezes UODO w swoich wytycznych z dnia 4 maja 2020 r. uznał, że wykorzystywanie dokumentacji w formie papierowej nie jest uzasadnione, jeżeli pracodawca:

– wdrożył elektroniczny obieg dokumentów, a pracownik ma bezpieczny dostęp do niezbędnych do pracy danych osobowych przy pomocy środków komunikacji elektronicznej,

– ma możliwość szybkiego, sprawnego i bezpiecznego wdrożenia elektronicznego obiegu dokumentacji,

– może udostępnić pracownikowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów[54].

Mając na uwadze powyższe oraz odpowiedni system zastępstw wprowadzony zakaz wynoszenia przez pracowników poza siedzibę pracodawcy jakichkolwiek dokumentów (co wiążę się z ryzykiem jej zagubienia, zniszczenia oraz dostępu osób nieuprawnionych), wydaje się to być zasadne rozwiązanie.

Zakończenie

Wykonywanie pracy poza siedzibą pracodawcy z wykorzystaniem urządzeń mobilnych nie jest nową metodą w polskim porządku prawnym w związku z wcześniej obowiązującymi przepisami dotyczącymi wykonywania telepracy, najczęściej wykorzystywanymi przez sektor prywatny. Dane Eurostatu za lata 2009–2019 pozwalają zauważyć wzrost liczby osób wykonujących pracę z domu. Z badań tych wynika, że „czasami" praca z domu wykonywana była przez 8,1% zatrudnionych w 2009 r., rosnąc do 10,8% w 2019 r. Stan ten w Polsce uległ zmianie w związku z ogłoszeniem epidemii COVID-19. Według danych Głównego Urzędu Statystycznego (dalej jako GUS) na koniec marca 2020 r. udział osób, które pracowały zdalnie, w ogólnej liczbie pracujących wyniósł 11,0%. Ta forma pracy była stosowana dwa razy częściej w sektorze publicznym (18% pracowników) niż prywatnym. Według GUS na koniec czerwca 2020 r. pracą zdalną objętych zostało 10,2% pracujących. Zmieniła się jednak skala wykorzystania pracy zdalnej w podmiotach prywatnych (ponad 9%) i publicznych (ok. 11,5%). Z kolei w trzecim kwartale, wraz z poluzowaniem obostrzeń pandemicznych, odsetek osób pracujących zdalnie spadł do 5,8%. Co ciekawe,

[52] S. Czub-Kiełczewska, op. cit.

[53] J. Marciniak, *Praca zdalna*.

[54] M. Rabe-Kozłowska, *Nowe wytyczne UODO dotyczące pracy zdalnej*, https://iodkancelaria.pl/2020/05/05/nowe-wytyczne-uodo-dotyczace-pracy-zdalnej/ (data dostępu: 13.11.2023).

skala wykorzystania pracy zdalnej w sektorze prywatnym (ponad 6,5%) była dwukrotnie wyższa niż w sektorze publicznym[55]. Według statystyk GUS na koniec grudnia 2022 r. było 422,6 tys. osób, które pracowały zdalnie w związku ze stanem zagrożenia epidemicznego[56]. Obecnie ok. 70% pracowników pracuje w biurze albo w pełnym wymiarze, albo w modelu hybrydowym, a jedynie 30% pracuje w pełni zdalnie[57]. Za jej wprowadzeniem przemawiają głównie korzyści finansowe pracodawcy związane z utrzymaniem pomieszczeń i oszczędności pracowników w zakresie kosztów i czasu dojazdów do pracy, ale również zwiększenie bezpieczeństwa pracowników. Wśród barier, ale głównie w sektorze publicznym, zauważyć należy kwestię dotyczącą specyfiki realizowanych zadań (tj. obsługa klientów) czy brak odpowiedniego wyposażenia podmiotów publicznych w sprzęt komputerowy oraz brak odpowiedniego przygotowania pracowników do wykonywania pracy zdalnej adekwatnie do zagrożeń. Jednakże głównym ryzykiem związanym z wykonywaniem pracy na odległość był brak odpowiednich zasad i procedur lub ich niezgodność z przepisami powszechnie obowiązującego prawa, w tym brak odpowiedniej świadomości kierownictwa oraz pracowników w tym zakresie. Kolejnym problemem był brak stosownych rozwiązań technicznych i organizacyjnych oraz brak zapewnienia ciągłości działania, szczególnie w sektorze publicznym. Powyższe mogło powodować zagrożenia związane z możliwością wycieku danych, utraty posiadanych zasobów oraz dostępu do danych osób nieuprawnionych.

W artykule podkreślono, że wcześniej, jeszcze przed pandemią, wielu administratorów przewidywało wykonywanie pracy poza siedzibą pracodawcy w związku z telepracą wykorzystywaną zarówno w sektorze prywatnym, jak i publicznym. Taka praktyka funkcjonowała w szczególności w sektorze prywatnym. Z kolei w sektorze publicznym w związku z pandemią koronawirusa wiele urzędów nie posiadało rozwiązań zarówno technicznych, jak i organizacyjnych do rozpoczęcia pracy w formie zdalnej, co nie oznacza, że nie było przyjętych dobrych praktyk w wielu instytucjach w tym zakresie, gdzie istniały rozwiązania oparte o procedury i mechanizmy funkcjonujące w związku ze świadczeniem przez pracowników telepracy. Ustawodawca już na etapie wdrażania instytucji telepracy nałożył na pracodawcę wiele istotnych obowiązków, tj. obowiązek ustalenia zasad ochrony danych przekazywanych telepracownikowi oraz przeprowadzania – w miarę potrzeby – instruktażu i szkolenia w tym zakresie. Przepisy dotyczące telepracy dawały również możliwość prze-

[55] J. Unterschütz, op. cit., s. 16–17.

[56] Główny Urząd Statystyczny, *Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce w czwartym kwartale 2022 roku*, https://stat.gov.pl/obszary-tematyczne/rynek-pracy/popyt-na-prace/wplyw-epidemii-covid-19-na-wybrane-elementy-rynku-pracy-w-polsce-w-czwartym-kwartale-2022-roku,4,12.html (data dostępu: 8.07.2024).

[57] Z. Biskupski, *Praca zdalna 2024. Biura nie pójdą do likwidacji, bo tylko co piąty pracownik chce pracować zdalnie*, https://kadry.infor.pl/wiadomosci/6436116,praca-zdalna-2024-biura-nie-pojda-do-likwidacji-bo-tylko-co-piaty-pra.html (data dostępu: 8.07.2024).

prowadzenia kontroli wykonywania przez pracownika telepracy w domu telepracownika, jednak musiała ona być zapowiedziana i odbywać się za jego zgodą. Pandemia COVID-19 stała się zatem dla pozostałych jednostek przyczyną rozwoju i wdrożenia pracy zdalnej, a znowelizowane przepisy prawa pracy w połączeniu z wymogami wynikającymi z art. 5, 24, 29 i 32 RODO stanowią podstawowe źródło warunków i zasad jej funkcjonowania. Należy podkreślić, że rozwój ten nie byłby możliwy także bez fachowego wsparcia doświadczonego IOD, który już na etapie funkcjonowania telepracy odpowiadał za odpowiednie działania uświadamiające poprzez wskazywanie istotnych ryzyk i zagrożeń związanych z wykonywaniem telepracy i bezpiecznych zasad jej świadczenia oraz monitorował jej prawidłowe funkcjonowanie.

Wskazane procedury w zakresie bezpieczeństwa i ochrony danych podczas wykonywania pracy w formie zdalnej, jak również zasady kontroli wykonywania pracy przez pracownika wykonującego zawiera się zazwyczaj w formie porozumienia zawieranego między pracodawcą i zakładową organizacją związkową lub w regulaminie. IOD powinien dokonać analizy obowiązujących w tym zakresie polityk i procedur wynikających m.in. z polityki bezpieczeństwa informacji, regulaminu pracy, a także udzielić niezbędnych wskazówek i wytycznych w celu dostosowania ich do obowiązujących przepisów i aktualnych zagrożeń. Niezwykle istotne jest przeprowadzenie przez IOD stosownych instruktaży/szkoleń, weryfikacja znajomości przez pracowników zasad i procedur dotyczących bezpieczeństwa informacji i ochrony danych osobowych podczas wykonywania pracy zdalnej adekwatnie do zidentyfikowanych ryzyk i aktualnych zagrożeń w obszarze bezpieczeństwa informacji. Zadaniem IOD jest również kontrola przestrzegania zasad i procedur związanych z funkcjonowaniem pracy zdalnej z istniejącymi zagrożeniami w tym zakresie, w tym zasad zgłaszania nieprawidłowości, obsługi incydentów i naruszeń ochrony danych, czy reagowania na żądania osób, których dane dotyczą. Czynności monitorujące i uświadamiające IOD powinny opierać się w szczególności o obowiązek zapewnienia:

– wszystkim pracownikom korzystania w pracy zdalnej ze sprzętu służbowego, w tym z Internetu (modemy/routery wraz z kartami SIM) zapewnionego przez pracodawcę. Dobrym rozwiązaniem w celu zapewnienia rozliczalności jest stosowanie z pracownikiem umowy o odpowiedzialności materialnej za powierzone mienie z uwzględnieniem postanowień dotyczących zasad bezpiecznego użytkowania sprzętu (bez względu na rodzaj sprzętu, tj. laptop, modem, router czy karta SIM), a także odpowiedzialności za sprzęt i dane na nim zawarte,

– szyfrowania wszelkich urządzeń mobilnych i nośników danych opuszczających siedzibę pracodawcy,

– właściwych warunków umożliwiających pracownikowi realizację zadań zgodnie z zasadą poufności i ochrony przed dostępem osób nieuprawnionych,

– zakazu podejmowania pracy zdalnej w miejscach publicznych,

– komunikowania się z pracodawcą i innymi pracownikami przy użyciu dedykowanych narzędzi służbowych, oraz stosowania środki technicznych i organizacyjnych wdrożonych w organizacji, tj. VPN, wieloskładnikowe uwierzytelnianie, szyfrowanie, pseudonimizacja,

– przestrzegania zakazu instalowania przez pracowników aplikacji i oprogramowań na urządzeniach służbowych,

– zabezpieczenia silnym hasłem prywatnych sieci internetowych używanych w celach służbowych,

– szyfrowania przez pracowników przesyłanych wiadomości poczty elektronicznej oraz zakaz korzystania z prywatnych skrzynek dla celów służbowych lub przesyłania tam jakichkolwiek danych służbowych,

– zgłaszania incydentów ochrony danych zgodnie z przyjętymi zasadami w organizacji,

– zakazu wynoszenia przez pracowników jakichkolwiek dokumentów papierowych poza siedzibę pracodawcy.

Powyższe zasady powinny zostać udokumentowane w postaci oświadczeń o zapoznaniu się z zasadami wykonywania pracy zdalnej oraz zachowania poufności przez pracowników, które powinny się znaleźć w aktach osobowych przed rozpoczęciem świadczenia pracy zdalnej przez pracownika. Należy pamiętać, że nie można poprzestać na jednorazowym działaniu zapewniającym czy wdrożeniu procedur, ale cały czas aktualizować obowiązujące polityki do zidentyfikowanych oraz aktualnych ryzyk i zagrożeń w obszarze cyberbezpieczeństwa, tak jak działalność doradcza i monitorująca inspektora nie może być traktowana jako działanie jedynie doraźne.

Wykaz literatury

Baranowska I., *Nowelizacja kodeksu pracy – praca zdalna i badanie trzeźwości pracowników*, 2021, Lex.

Biskupski Z., *Praca zdalna 2024. Biura nie pójdą do likwidacji, bo tylko co piąty pracownik chce pracować zdalnie*, https://kadry.infor.pl/wiadomosci/6436116,praca-zdalna-2024-biura-nie-pojda-do-likwidacji-bo-tylko-co-piaty-pra.html.

Czub-Kiełczewska S., *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej*, 2020, Lex.

Delegatura Najwyższej Izby Kontroli w Białymstoku, *Organizacja pracy zdalnej w wybranych podmiotach wykonujących zadania publiczne w związku z ogłoszeniem stanu epidemii*, NIK, Warszawa 2021.

Delegatura Najwyższej Izby Kontroli w Olsztynie, *Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych*, NIK, Warszawa 2022.

Główny Urząd Statystyczny, *Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce w czwartym kwartale 2022 roku*, https://stat.gov.pl/obszary-tematyczne/rynek-pracy/popyt-na-prace/wplyw-epidemii-covid-19-na-wybrane-elementy-rynku-pracy-w-polsce-w-czwartym-kwartale-2022-roku,4,12.html.

Gruca K., *Sprzęt służbowy używany przez pracownika do celów prywatnych*, https://poradnikprzedsiebiorcy.pl/-sprzet-sluzbowy-uzywany-przez-pracownika-do-celow--prywatnych.

Hady-Głowiak S., Kozłowski D., *Dekalog ochrony danych osobowych – stosowanie zasad przetwarzania danych osobowych jako podstawa bezpieczeństwa przetwarzania danych*, [w:] J. Wołejszo, K. Rejman, M. Wilczyńska (red.), *Bezpieczeństwo informacji w organizacjach*, Kaliskie Tow. Przyjaciół Nauk, Kalisz 2021.

Horbaczewski R., *Gdy urzędnik pracuje w domu, hakerowi łatwiej wejść do urzędu*, 2022, Lex.

Jagiełło-Jaroszewska E., *Ochrona danych osobowych a telepraca i praca zdalna*, [w:] D. Dörre-Kolasa (red.), *Ochrona danych osobowych w zatrudnieniu*, C.H. Beck, Warszawa 2020.

Janik M., Hady-Głowiak S., *Bezpieczeństwo informacji jako zadanie jednostek sektora finansów publicznych*, „Studia Prawnoustrojowe" 2023, nr 62.

Kryczka S., *Praca zdalna pod kontrolą Państwowej Inspekcji Pracy*, 2020, Lex.

Krzyszkowska-Dąbrowska M., *Praca zdalna. Praktyczny przewodnik*, Wolters Kluwer, Warszawa 2020.

Kuba M., *Ochrona danych osobowych w kontekście pracy zdalnej – wybrane zagadnienia*, [w:] M. Mędrala (red.), *Praca zdalna w polskim systemie prawnym*, 2021, Lex.

Marciniak J., *Praca zdalna – aspekty prawne*, [w:] J. Marciniak (red.), *Praca zdalna i hybrydowa. Aspekty organizacyjne i prawne*, 2023, Lex.

Marciniak J., *Praca zdalna*, 2020, Lex.

Mędrala M., *Praca zdalna. Komentarz do nowelizacji Kodeksu pracy*, 2023, Lex.

Mędrala M., *Praca zdalna w administracji*, 2023, Lex.

Nowicka M., *Telepraca – forma elastycznego zatrudnienia*, 2023, Lex.

Nowicki A., *Praca zdalna a telepraca – czym się różnią?*, https://kadry.infor.pl/kadry/inne_formy_zatrudnienia/telepraca/4710942,Praca-zdalna-a-telepraca-czym-sie--roznia.html.

Prasolek Ł., A. Kiełbratowska A., *Praca zdalna w praktyce. Zagadnienia prawa pracy i RODO*, [w:] Ł. Prasołek (red.), *Pomoc dla pracodawcy w sprawach pracowniczych w dobie kryzysu. Tarcza antykryzysowa, prawo pracy, RODO, ZUS, PIT*, C.H. Beck, Warszawa 2020.

Rabe-Kozłowska M., *Nowe wytyczne UODO dotyczące pracy zdalnej*, https://iodkancelaria.pl/2020/05/05/nowe-wytyczne-uodo-dotyczace-pracy-zdalnej/.

Sakowska-Baryła M., *Ochrona danych osobowych w warunkach pracy zdalnej*, Wolters Kluwer, Warszawa 2020.

Unterschütz J., *Pojęcia telepracy i pracy zdalnej. dotychczasowe doświadczenia i regulacje prawne*, [w:] M. Mędrala (red.), *Praca zdalna w polskim systemie prawnym*, 2021, Lex.

Summary

Selected legal and practical aspects of data protection related to the performance of remote work

Keywords: law, data protection, remote working, teleworking, Data Protection Officer, security information.

The subject of this article is to present the issue related to the evolution of the operation of telework and the legal and practical aspects concerning personal data protection and its implementation from the operation of telework to the performance of remote work, bearing in mind the period of the COVID-19 pandemic and the increased risk of incidents and violations. The performance of "remote" work is nothing new in the Polish legal order, and statistics show that its performance has increased slightly since 2009, mainly in the private sector. The purpose of the article is also to try to answer the question of whether the performance of remote work represents an opportunity or a threat to the employer in terms of the effective and efficient performance of tasks by subordinate employees adequate to the risks in cyberspace. The article points out the opportunities and risks associated with the introduction of this form of work provision. The main arguments in favour of its introduction are the employer's financial benefits related to the maintenance of the premises and the savings of employees in terms of costs and commuting time, but also the increased safety of employees. Among the barriers occurring mainly in the public sector, one should note the issue related to the specificity of the tasks performed (i.e. customer service), or the lack of adequate equipment of public entities with computer equipment, as well as the lack of proper preparation of employees to perform remote work adequate to identified and current risks. The article highlights the role of the controller and processor to properly and promptly involve the Data Protection Officer (hereinafter referred to as DPO) in all matters concerning the implementation and evaluation of the functioning of the rules and procedures, tools and conditions for the safe provision of remote work adequately to the risks, taking into account the requirements outlined in, among others, Articles 24, 29 and 32 of the GDPR, as well as continuous legislative or organizational changes. Significant attention was paid to the awareness-raising activities and the duties of the DPO to provide the necessary guidance, followed by his monitoring role to assess the implementation of the implemented rules for the performance of remote work, considering compliance with security information and protection requirements, including procedures and rules for reporting any incidents and violations.