# RODO znów wchodzi do kodeksu pracy. Zmiany obejmą też systemy elektroniczne

Polski ustawodawca uchwalił ustawę z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. poz. 730) – dalej jako: **ustawa wdrożeniowa** lub **ustawa wprowadzająca RODO**. Celem ustawy – jak sama jej nazwa wskazuje – jest zharmonizowanie przepisów poszczególnych ustaw krajowych z regulacjami wynikającymi z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 – dalej jako: **RODO**, które obowiązuje w polskim porządku prawnym od 25 maja 2018 r. Polski ustawodawca za pośrednictwem ustawy wdrażającej zdecydował się na dokonanie nowelizacji aż 162 ustaw. Tak obszerne zmiany wynikają z konieczności dostosowania polskich przepisów do postanowień RODO. Zmiany dotykają także sektora pracy – dotyczą one m.in. określenia podstaw prawnych przetwarzania danych osobowych, wskazania kategorii danych osobowych, które są niezbędne do pozyskania przez pracodawcę w związku z podejmowaniem przez niego działań przed zawarciem umowy o pracę oraz po jej zawarciu, uregulowania kwestii przetwarzania danych wrażliwych, w tym możliwości pobierania danych biometrycznych od pracownika, stosowania monitoringu czy przetwarzania danych związanych z realizacją świadczeń z zakładowego funduszu świadczeń socjalnych. Znowelizowane przepisy zaczną obowiązywać w terminie 14 dni od dnia ogłoszenia ich w Dzienniku Ustaw, tj. od 4 maja 2019 r.

## I. PROWADZENIE PROCESU REKRUTACJI

### Co można pozyskać od kandydata do pracy

Ustawa wdrożeniowa wprowadzi zmiany w zakresie danych, jakich pracodawca może domagać się od kandydatów do pracy w toku prowadzonych procesów rekrutacji w firmie. Po wejściu w życie znowelizowanego art. 22[1] par. 1 kodeksu pracy, pracodawca będzie mógł zażądać od kandydata następujących informacji:

a) imię (imiona) i nazwisko kandydata,
b) datę urodzenia,
c) dane kontaktowe wskazane przez kandydata,
d) wykształcenie,
e) kwalifikacje zawodowe,
f) przebieg dotychczasowego zatrudnienia.

W dotychczasowym brzmieniu ww. przepisu, pracodawca mógł pozyskiwać od kandydata dodatkowo dane osobowe takie jak: imiona rodziców oraz miejsce zamieszkania (adres do korespondencji). Ustawodawca zdecydował jednak, że ww. dane osobowe nie są niezbędne pracodawcy w celu prowadzenia procesu rekrutacji, wobec czego postanowił wykreślić ten zakres danych z kodeksu pracy. Oczywiście kandydat

będzie mógł samodzielnie w CV wskazać swój adres zamieszkania, jednak fakt jego niepodania nie może rodzić negatywnych skutków dla tej osoby, a pracodawca nie może tych danych od niego żądać. Co więcej, w zakresie danych w postaci wykształcenia, kwalifikacji zawodowych oraz przebiegu dotychczasowego zatrudnienia kandydata, pracodawca będzie mógł zażądać ich podania tylko wtedy, gdy jest to niezbędne do wykonywania pracy na określonym stanowisku. Natomiast żądanie innych danych od kandydata będzie co do zasady niedopuszczalne (patrz przykład 1 oraz ramki 1-2).

**Przykład 1**
**Zdjęcia w CV**

Dział HR spółki ABC sp. z o.o. w toku prowadzonego procesu rekrutacji wskazuje, że kandydaci powinni przesyłać dokumenty aplikacyjne zawierające ich zdjęcia, a CV bez zdjęć nie będą rozpatrywane. Czy od 4 maja 2019 r. pracodawca może tego żądać od kandydatów?
Z reguły kandydaci zamieszczają swoje fotografie w dokumentach aplikacyjnych. Robią to jednak najczęściej dobrowolnie. Natomiast zarówno dziś, jak i po wejściu w życie zmian do k.p., pracodawca nie może zmusić kandydata do przesłania zdjęcia, a brak dobrowolnego przesłania fotografii nie może rodzić negatywnych konsekwencji dla takiej osoby.

**Ramka 1**
**Kwestionariusze osobowe**

Istotną kwestią jest również to, że dotychczas działy personalne w firmach przy pozyskiwaniu danych od kandydatów do pracy, posiłkowały się wzorami, stanowiącymi załącznik do rozporządzenia ministra pracy i polityki socjalnej z 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (t.j. Dz.U. z 2017 r. poz. 894). Załącznik nr 1 do ww. rozporządzenia zawierał kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie. W kwestionariuszu tym zakres zbieranych od kandydatów danych osobowych obejmował m.in.: imię i nazwisko kandydata, imiona rodziców, obywatelstwo, miejsce zamieszkania, wykształcenie, wykształcenie uzupełniające, przebieg zatrudnienia, dodatkowe uprawnienia, umiejętności i zainteresowania. Jednocześnie pkt 10 kwestionariusza zawierał oświadczenie, że podane przez kandydata dane osobowe są zgodne z jego dokumentem tożsamości – w tym miejscu wymagano podania numeru i serii dowodu osobistego. Oczywiście pracodawcy nie mieli obowiązku korzystania z przygotowanego przez ustawodawcę kwestionariusza, jednak z praktyki wiadomo, że często z takiego rozwiązania korzystali.
Po wejściu w życie RODO tj. po 25 maja 2018 r. ww. rozporządzenie z 1996 r. nie zostało dostosowane do RODO. Zamiast tego ustawodawca uchwalił nowe, tj. rozporządzenie ministra pracy i polityki społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej (Dz.U. poz. 2369) dopiero kilka miesięcy po wejściu w życie RODO – zaczęło ono obowiązywać 1 stycznia 2019 r. Jak już wspomniano, z uwagi na to, że pracodawcy chętnie korzystali z przygotowanych przez ustawodawcę kwestionariuszy osobowych,

zbierane były również numery dowodów osobistych. Po wejściu w życie RODO, z uwagi m.in. na zasadę minimalizacji danych, a także brak przepisów uzasadniających przetwarzanie przez pracodawców numerów dokumentów ich tożsamości, korzystanie z kwestionariuszy osobowych oznaczało, że pracodawca w rzeczywistości naruszał przepisy RODO. Od 25 maja 2018 r. zbieranie i przetwarzanie danych z dokumentów tożsamości kandydatów do pracy jest bowiem sprzeczne z przepisami dot. ochrony danych osobowych. Obecnie, w przypadku wykorzystywania w toku rekrutacji kwestionariusza stanowiącego załącznik nr 1 do ww. rozporządzenia z 1996r., konieczne jest wykreślenie pkt 10 w zakresie zbierania numeru i serii dowodu osobistego.

**Ramka 2**
**Pytanie o karalność**

Do czasu wejścia w życie RODO dość powszechną praktyką było żądanie od kandydatów danych o niekaralności przyszłych pracowników. Przetwarzanie takich danych osobowych kandydata możliwe jest jedynie wtedy, gdy przepis prawa przewiduje obowiązek ich żądania przez pracodawcę (tak np. ustawa z 21 listopada 2008 r. o służbie cywilnej, t.j. Dz.U. 2018 r. poz 1559). W zakresie legalizacji zbierania danych o niekaralności dyskusyjne jest, czy możliwe jest również powoływanie się na to, że kandydat wyraził zgodę na przetwarzanie jego danych dotyczących karalności. W naszej ocenie nie ma możliwości zbierania danych o karalności na podstawie zgody. W przeciwnym razie istniałoby duże ryzyko, że przyszli pracodawcy korzystaliby z tego rozwiązania w sposób nadmiarowy z uwagi na ich uprzywilejowaną pozycję oraz nierówność stron stosunku pracy.

**Zgodnie z przepisami**

Aby można było stwierdzić, że proces rekrutacji w firmie przebiega prawidłowo, niezbędne jest istnienie odpowiedniej podstawy przetwarzania danych osobowych w przepisach prawa. Taką podstawą w RODO jest m.in. zgoda kandydata (art. 6 ust 1 lit a). Powtarza ją również nowy art. 22[1a] k.p. przewidując przetwarzanie w oparciu o nią danych wybiegających poza opisany wyżej zakres z art. 22[1] k.p. Ponadto, zgodnie z nowym art. 22[1b] par. 1 k.p. w przypadku danych szczególnej kategorii zgoda może stanowić podstawę przetwarzania takich danych przez pracodawcę (określonych w art. 9 RODO), wyłącznie wtedy, gdy ich przekazanie następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika.
Przypomnijmy przy tym, że oprócz konieczności wykazania, że kandydat wyraził zgodę na przetwarzanie jego danych osobowych – zgodnie z zasadą rozliczalności – na przyszłym pracodawcy ciąży szereg obowiązków związanych z przetwarzaniem takich danych. Mianowicie, prowadzenie procesu rekrutacji zgodnie z RODO wymaga:

1. uzyskania zgody kandydata na przetwarzanie jego danych osobowych – zgodnie ze stanowiskiem UODO, podzialanym przez autorów niniejszego opracowania. Wskazać jednak trzeba na odmienne stanowisko Ministerstwo Cyfryzacji, które w objaśnieniach prawnych z 23 stycznia 2019 r. wskazuje, że w przypadku prowadzenia rekrutacji na konkretne stanowisko nie jest wymagana zgoda, gdyż

podstawą przetwarzania jest dążenie do zawarcia umowy, tj. art. 6 ust 1 lit b) RODO.
2. uzyskania zgody kandydata na przetwarzanie jego danych osobowych w ramach przyszłych procesów rekrutacji (jeżeli tego dotyczy),
3. wypełnienia obowiązku informacyjnego określonego w art. 13 lub 14 RODO (w zależności od sposobu prowadzenia procesu rekrutacji),
4. zebrania danych osobowych zgodnie z zasadą minimalizacji i obowiązującymi przepisami (w szczególności zgodnie ze znowelizowanym art. 22[1] k.p.),
5. przyjęcia odpowiednich procedur organizacyjnych w zakresie postępowania z danymi osobowymi kandydatów – w szczególności w zakresie terminu usuwania danych,
6. wdrożenia odpowiednich zabezpieczeń w systemach, w których są przetwarzane dane i dostosowanie ich do RODO.

## II. PRZETWARZANIE DANYCH PRACOWNIKÓW

Ustawa wdrożeniowa wprowadza zmiany dotyczące przetwarzania danych osobowych pracowników. Obejmują one zwłaszcza doprecyzowanie rodzaju danych, jakie pracodawca może przetwarzać, w tym danych biometrycznych, a także stosowania monitoringu w zakładzie pracy. Wskazać jednak trzeba, że przed uchwaleniem ustawy wdrożeniowej, zmianie uległ szereg innych ustaw i aktów wykonawczych, które określają sposób postępowania z danymi osobowymi pracowników. Dotyczy to m.in. ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000), która wprowadziła zmiany do kodeksu pracy – obowiązujące od 25 maja 2018 r., a także rozporządzenia ministra rodziny, pracy i polityki społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej (Dz.U. poz. 2369), które obowiązuje od 1 stycznia 2019 r. Oczywiście pracodawcy od 25 maja 2018 r. zobowiązani są również bezpośrednio stosować przepisy RODO.

### Rodzaj zbieranych informacji

Z art. 22[1] par. 1 k.p. w nowym brzmieniu, wynika, że pracodawca może przetwarzać następujący rodzaj danych pracowników, przy czym jest to taki sam zakres jak w przypadku kandydatów ():

a) imię (imiona) i nazwisko,
b) datę urodzenia,
c) dane kontaktowe wskazane przez pracownika,
d) wykształcenie,
e) kwalifikacje zawodowe,
f) przebieg dotychczasowego zatrudnienia.

Ponadto – zgodnie ze znowelizowanym art. 22[1] par. 3 k.p. – pracodawca może przetwarzać następujące dane osobowe pracowników:

a) adres zamieszkania,
b) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość,

c) inne dane osobowe pracownika, a także dane osobowe jego dzieci i innych członków najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
d) wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie,
e) numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Pracodawca będzie miał obowiązek zbierania wyłącznie następujących danych: imię i nazwisko, nr PESEL, data urodzenia, adres zamieszkania i dane kontaktowe pracownika, a co do pozostałych danych – będzie mógł je gromadzić fakultatywnie. Przykładowo, dane takie jak wykształcenie, kwalifikacje zawodowe i przebieg dotychczasowego zatrudnienia pracodawca będzie mógł pozyskać, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku. Ponadto pracodawca na podstawie art. 22[1] par. 4 k.p. będzie mógł przetwarzać inne niż wskazane powyżej dane osobowe pracowników, jeżeli okaże się to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Pracodawca jako administrator danych osobowych pracowników ma obowiązek do zrealizowania wobec nich obowiązku informacyjnego tj. przedstawienia zasad przetwarzania ich danych osobowych. Wydawać by się mogło, że jedyną podstawą przetwarzania danych osobowych pracowników jest umowa, jednak tych podstaw jest zdecydowanie więcej. Na pracodawcy ciąży obowiązek precyzyjnego wskazania w treści obowiązku informacyjnego ich wszystkich (patrz ramka 3).

Artykuł 13 RODO wyczerpująco wskazuje, jakie informacje powinny znaleźć się w treści obowiązku informacyjnego. Pomimo tego, pracodawcy często mają problem z jego realizacją. Z reguły najbardziej problematyczną kwestią jest dla nich:

1) wskazanie podstaw przetwarzania danych pracowników, a także
2) forma wypełnienia tego obowiązku.

**Ramka 3**
**Poinformowanie pracownika**

Można wyróżnić następujące podstawy prawne przetwarzania danych osobowych pracowników:

- art. 6 ust 1 lit a RODO – podstawą prawną jest zgoda; dotyczy to sytuacji, gdy pracodawca przetwarza dane osobowe w postaci wizerunku pracowników albo zakres przetwarzanych danych jest szerszy niż z art. 22[1] par. 1 i 3 znowelizowanego k.p.,
- art. 6 ust 1 lit b) RODO – podstawą prawną jest umowa,
- art. 6 ust. 1 lit. c) RODO – podstawą prawną jest obowiązek prawny ciążący na administratorze; dotyczy to realizacji prawa pracy, przepisów księgowych itp.,
- art. 6 ust 1 lit. f) RODO – podstawą prawną jest prawnie uzasadniony interes administratora; dotyczy to sytuacji zainstalowania na terenie zakładu pracy monitoringu, prowadzenia czynności archiwizacyjnych czy raportowych, a także przekazywania danych w ramach grup kapitałowych.

Z kolei w zakresie przetwarzania przez pracodawcę danych szczególnej kategorii, wyróżnić można następujące podstawy prawne:

- art. 9 ust 2 lit a) RODO – podstawą prawną jest zgoda na przetwarzanie tych danych osobowych,
- art. 9 ust. 2 lit. b) RODO – podstawą prawną jest wypełnienie obowiązków i wykonywanie szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej.

Oczywiście, w zależności od działalności pracodawcy i sposobu postępowania z danymi pracowników, być może konieczne będzie wskazanie w treści obowiązku informacyjnego kierowanego do pracowników także podstaw przetwarzania innych niż wymienione powyżej.

Jedną z podstaw przetwarzania danych osobowych pracowników jest – i po 4 maja nadal będzie – zgoda. Nowy art. 22[1a] par. 2 k.p. stanowi, że brak zgody pracownika na przetwarzanie jego danych osobowych lub jej wycofanie, nie może być podstawą niekorzystnego traktowania jego osoby, a także nie może powodować wobec niego jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę. Takie stanowisko było już wcześniej przedmiotem zainteresowania sądów, które na gruncie przepisów obowiązujących jeszcze przed wejściem w życie RODO wskazywały na brak równowagi w relacji pracownik – pracodawca, co może stanowić podstawę do wykorzystywania w sposób nieprawidłowy dobrowolności przetwarzania danych osobowych na podstawie zgody. Z tego względu wprowadzenie powyższego przepisu należy ocenić pozytywne.

Kolejnym problemem, z jakim spotykają się pracodawcy, jest forma wypełnienia obowiązku informacyjnego. Przepisy nie wskazują, w jaki sposób należy poinformować osoby o sposobie przetwarzania ich danych osobowych. W tym zakresie trzeba mieć jednak na uwadze zasadę rozliczalności, która wprowadza wymóg udowodnienia, że obowiązek ten został zrealizowany. Z tego względu pracodawca w prowadzonej przez siebie ewidencji powinien posiadać dowód, że pracownicy zapoznali się z obowiązkiem informacyjnym. W tym zakresie najbezpieczniejszą formą zrealizowania obowiązku informacyjnego będzie sporządzenie jego treści na piśmie, a następnie wręczenie każdemu pracownikowi wraz z poświadczeniem otrzymania. Obowiązek informacyjny może też stanowić załącznik do umowy o pracę (patrz przykłady 2-3).

**Przykład 2**
**Konieczna zgoda**

Pan Łukasz został zatrudniony 1 stycznia 2019 r. na stanowisku sprzedawcy. Poza danymi osobowymi pozyskanymi na etapie rekrutacji, pan Łukasz dodatkowo przekazał pracodawcy – na jego żądanie – swój prywatny adres email i numer telefonu, które zostały zamieszczone na stronie internetowej pracodawcy. Pan Łukasz nie wyraził jednak w żaden sposób zgody na przetwarzanie jego danych osobowych w postaci prywatnego numeru telefonu i prywatnego adresu e-mail. W tym zakresie, pracodawca powinien uzyskać od niego zgodę na przetwarzanie ww. danych osobowych.

**Przykład 3**
**Sposób realizacji obowiązku**

Pracodawca sporządził treść obowiązku informacyjnego o przetwarzaniu danych osobowych pracowników, którą zamieścił na tablicy w sekretariacie prezesa zarządu. Pracownicy mieli możliwość zapoznania się z treścią przygotowanego dokumentu tylko wtedy, gdy pojawiali się w sekretariacie. Przy czym większość zatrudnionych nie posiadała informacji, że obowiązek informacyjny się tam znajduje, a w sekretariacie prezesa zarządu przebywała zazwyczaj wyłącznie kadra kierownicza, a szeregowi pracownicy nie mieli zasadniczo do niego dostępu. W takiej sytuacji pracodawca nieprawidłowo wypełnił obowiązek poinformowania pracowników o przetwarzaniu ich danych osobowych, bowiem większość z nich nie miała możliwości zapoznania się z tym dokumentem.

## Tylko przez upoważnione osoby

W nowym brzmieniu art. 22[1b] par. 3 k.p. stanowi, że do przetwarzania danych szczególnej kategorii mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę oraz że są one zobowiązane do zachowania ich w tajemnicy. Co istotne, nie dotyczy to wyłącznie danych szczególnej kategorii. Każda osoba, która w imieniu pracodawcy jest dopuszczona do pracy z danymi pracowników – bez względu na to, czy stanowią one dane wrażliwe, czy zwykłe – powinna posiadać pisemne upoważnienie wydane przez pracodawcę do ich przetwarzania.

## Dane o przewinieniach pracowników

Pracodawca może przetwarzać dane dotyczące karalności pracowników, gdy przepisy prawa tak stanowią. Możliwość przetwarzania tych danych na innej podstawie jest jednak dyskusyjna. Pracodawca nie może zatem żądać od pracowników przestawienia tych danych w sposób dowolny (patrz przykład 4). Przykładowo może żądać przedstawienia takich danych w następujących sytuacjach:

1. w przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku – wówczas operator infrastruktury krytycznej żąda od pracownika lub ww. osoby przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym (ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, t.j. Dz.U. z 2018 r. poz. 1401 ze zm.),
2. w przypadku podmiotów zatrudnionych na niektórych stanowiskach w podmiotach sektora finansowego zgodnie z ustawą z 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego (Dz.U. poz. 1130),

3. w przypadku osób ubiegających się o stanowisko pracownika ochrony zgodnie z art. 19 ust. 1 pkt. 7 ustawy z 22 sierpnia 1997 r. o ochronie osób i mienia (t.j. Dz.U. z 2018 r. poz. 2142).

**Przykład 4**
**Wymóg dla kierownika**

Pan Wojciech jest zatrudniony na stanowisku sprzedawcy w firmie deweloperskiej. Pracodawca postanowił awansować go na stanowisko kierownika, jednak możliwość otrzymania awansu uzależnił od przedstawienia przez Pana Wojciecha danych o niekaralności, motywując to tym, że pracownik będzie posiadał dostęp do dokumentów finansowych spółki. Pan Wojciech nie ma obowiązku przedstawienia danych o jego karalności, a pracodawca nie może ich żądać, ponieważ żaden przepis prawa nie stanowi o tym, aby osoby pełniące funkcje kierownicze zobowiązane były do przedstawienia danych o niekaralności.

**Wizerunek pracownika**

Pracodawca może przetwarzać dane osobowe w postaci wizerunku pracownika, jednak musi posiadać jego zgodę na to, która w tym przypadku jest podstawą przetwarzania (art. 6 ust. 1 lit. a) RODO). Wizerunek pracowników może być przetwarzany w rozmaity sposób np. zamieszczany na stronie internetowej firmy, na identyfikatorach albo w social mediach pracodawcy. Zgoda pracownika jest konieczna niezależnie od sposobu przetwarzania zdjęć pracowników, przy czym najlepiej byłoby gdyby zatrudniony miał możliwość wyboru sposobu przetwarzania wizerunku (tj. aby mógł wyrazić odrębną zgodę na każdy ze sposobów przetwarzania). Istnieją jednak poglądy w doktrynie, że przetwarzanie wizerunku pracownika wewnątrz organizacji tj. na identyfikatorach lub w Intranecie powinno odbywać się nie na podstawie zgody, lecz prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit f) RODO). Dodatkowo, przetwarzanie wizerunku może mieć miejsce jeszcze na innej podstawie prawnej np. w przypadku, gdy przepisy prawa określają wzór identyfikatora ze zdjęciem (patrz przykład 5). Ponadto przetwarzanie wizerunku powoduje, że obowiązek informacyjny powinien być odpowiednio uzupełniony o tę kwestię. Jednocześnie należy pamiętać, że jeżeli przetwarzanie wizerunku pracowników zasadniczo odbywa się na podstawie zgody, to pracownik w każdym momencie może tę zgodę cofnąć, co będzie oznaczało dla pracodawcy konieczność zaprzestania przetwarzania danych w ten sposób. Natomiast jeżeli przetwarzanie danych odbywa się na innej podstawie niż zgoda, takie uprawnienie pracownikowi nie będzie przysługiwało.

**Przykład 5**
**Strona internetowa i nagrania video**

Pracodawca przetwarza wizerunek pracowników i umieszcza ich zdjęcia na swojej stronie internetowej. Na powyższe działanie posiada pisemną zgodę zatrudnionych. Na terenie zakładu jest również zainstalowany monitoring, za pomocą którego pracodawca także przetwarza wizerunek pracowników. Na takie działanie – wprowadzenie

monitoringu – nie jest konieczna zgoda pracownika, gdyż podstawą prawną przetwarzania danych za pośrednictwem nagrań video jest prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f) RODO).

**Monitoring w miejscu pracy**

Pracodawcy często instalują na terenie firmy monitoring, za pomocą którego przetwarzane są dane osobowe nie tylko pracowników lecz także osób trzecich np. klientów. W zakresie przetwarzania wizerunku pracowników i stosowania monitoringu odpowiednie zapisy w kodeksie pracy zostały wprowadzone już na podstawie wspomnianej wcześniej ustawy z 10 maja 2018 r. o ochronie danych osobowych, która weszła w życie 25 maja 2018 r. Aktualna pozostaje możliwość zastosowania monitoringu w sytuacji konieczności zapewnienia bezpieczeństwa pracowników, ochrony mienia lub kontroli produkcji bądź zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. W ustawie wdrożeniowej doprecyzowano, że instalacja monitoringu wizyjnego w pomieszczeniach sanitarnych, szatniach, stołówkach oraz palarniach wymaga uzyskania przez pracodawcę uprzedniej zgody zakładowej organizacji związkowej, a jeżeli taka organizacja u pracodawcy nie występuje – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przez niego przyjętym. Dodatkowo wskazano, że monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej.
Na podstawie przywołanej powyżej ustawy o ochronie danych osobowych, pracodawcy, którzy wykorzystują nagrania z monitoringu mają obowiązek:

- oznaczenia pomieszczeń i monitorowanego terenu w sposób widoczny i czytelny, za pomocą odpowiednich znaków (piktogramów) lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem,
- przetwarzania wizerunku utrwalonego na nagraniach wyłącznie do celów, dla których zostały zebrane i przechowywanie ich przez okres nieprzekraczający trzech miesięcy od dnia nagrania, chyba że mogą one stanowić dowód w postępowaniu prowadzonym na podstawie przepisów prawa,
- ustalenia celów, zakresu oraz sposobu zastosowania monitoringu w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu (jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy) – dodatkowo przed dopuszczeniem pracownika do pracy należy przekazać mu pisemną informację w tym zakresie,
- poinformować pracowników o wprowadzeniu monitoringu w sposób przyjęty u danego pracodawcy nie później niż dwa tygodnie przed jego uruchomieniem.

Z uwagi na to, że monitoring zainstalowany na terenie firmy obejmuje swym zasięgiem nie tylko pracowników, ale też osoby trzecie np. kontrahentów, konieczne będzie wypełnienie obowiązku informacyjnego w tym zakresie również wobec tych osób. W związku z tym, niezależnie od obowiązku odpowiedniego oznaczenia monitoringu za pomocą piktogramów, konieczne będzie także zamieszczenie w widocznym miejscu tablicy informacyjnej o przetwarzaniu danych osobowych za pomocą monitoringu, z którą będą mogły zapoznać się osoby wchodzące na teren firmy (w obszar monitorowany).

## Dane biometryczne

Zgodnie z definicją zawartą w art. 4 pkt. 14 RODO dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Bardzo często pojawia się wątpliwość, czy przetwarzanie wizerunku na podstawie fotografii oznacza przetwarzanie danych biometrycznych. Unijny prawodawca w motywie 51 RODO wyjaśnił jednak, że przetwarzanie fotografii nie zawsze będzie stanowić przetwarzanie szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją "danych biometrycznych" tylko wtedy, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.
Dane biometryczne stanowią dane szczególnej kategorii, a ich przetwarzanie co do zasady jest możliwe jeżeli zaistniała przesłanka określona w art. 9 ust. 2 RODO. W ustawie wdrożeniowej wskazano jednak, że pracodawca może być uprawniony do przetwarzania takich danych na podstawie zgody wyłącznie w przypadku, gdy ich przekazanie następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika (przy czym zgoda ta musi być dobrowolna, przykładowo pracodawca powinien zapewnić możliwość dostępu do pomieszczenia za pośrednictwem innych środków, takich jak karta magnetyczna). Ponadto, zgodnie z nowym art. 22[1b] par. 2 k.p. przetwarzanie danych biometrycznych pracownika będzie dopuszczalne, 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 (przy czym jest to uprawnienie pracodawcy). Jeżeli więc zaistnieje wskazana powyżej przesłanka, to przetwarzanie danych biometrycznych będzie możliwe bez konieczności odebrania zgody od pracownika.
Ustawodawca nie wskazał katalogu danych biometrycznych, jakie mogą być przetwarzane przez pracodawcę – z uwagi na postęp technologiczny jest to rozwiązanie słuszne. Zauważyć również trzeba, że wśród funkcjonujących na rynku systemów kontroli dostępu, funkcjonują również takie, które pozwalają na uzyskanie dostępu do pomieszczeń za pomocą odcisku palca, jednak w efekcie nie dochodzi do przetwarzania odwzorowań linii papilarnych (danych biometrycznych), tylko – zgodnie z zapewnieniami producentów – powstaje algorytm matematyczny. Przed skorzystaniem przez pracodawcę z takich systemów konieczna jest jednak uprzednia weryfikacja, czy rzeczywiście nie dochodzi do przetwarzania danych biometrycznych i czy w związku z tym nie ma konieczności zbierania zgód od pracowników.

## Nowy pracodawca a badania lekarskie

Od 4 maja zmianie ulegnie art. 229 par. 1[1] pkt 2 k.p., który dotyczy możliwości niekierowania nowoprzyjętych pracowników na badania lekarskie. Przepis ten został doprecyzowany w ustawie wdrażającej i zgodnie z jego nowym brzmieniem osoby przyjmowane do pracy na dane stanowisko u innego pracodawcy w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, jeżeli posiadają aktualne orzeczenie lekarskie stwierdzające brak przeciwwskazań do pracy w warunkach pracy

opisanych w skierowaniu na badania i pracodawca ten stwierdzi, że warunki te odpowiadają warunkom występującym na tym stanowisku pracy, nie muszą przechodzić badań lekarskich przed dopuszczeniem do pracy. Możliwość ta nie dotyczy jednak osób przyjmowanych do wykonywania prac szczególnie niebezpiecznych. Jednocześnie do art. 229 k.p. dodany zostanie par. 1[3], który stanowi, że pracodawca żąda od osoby, o której mowa w par. 1[1] pkt 2 oraz w par. 1[2], aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na danym stanowisku oraz skierowania na badania będącego podstawą wydania tego orzeczenia. Ustawa wdrażająca dodaje również par. 7[1] zgodnie z którym w przypadku stwierdzenia, że warunki określone w skierowaniu, o którym mowa w par. 1[3], nie odpowiadają warunkom występującym na danym stanowisku pracy, pracodawca zwraca osobie przyjmowanej do pracy to skierowanie oraz orzeczenie lekarskie wydane w wyniku tego skierowania.

**Ramka 4**
**Okres przechowywania**

1 stycznia 2019 r. weszły w życie znowelizowane przepisy kodeksu pracy, wprowadzone na podstawie ustawy z 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją (Dz.U. poz. 357), na podstawie których zmianie uległ okres przechowywania akt pracowniczych. Powyższe jest istotne z punktu widzenia obowiązków pracodawcy dotyczących okresu przetwarzania danych osobowych pracowników. Skrócenie okresu przechowywania akt pracowniczych dotyczy zwłaszcza pracowników zatrudnionych po 1 stycznia 2019 r. Natomiast dla zatrudnionych od stycznia 1999 r. do grudnia 2018 r., pracodawca ma możliwość skrócenia okresu przechowywania akt do 10 lat, jeżeli przekaże do ZUS oświadczenie (ZUS OSW) oraz raport informacyjny (ZUS RIA). W przypadku pracowników zatrudnionych przed 1 stycznia 1999 r., pracodawca nie ma możliwości skrócenia okresu przechowywania akt. W tym przypadku nadal należy stosować okres 50-letni.

Dopełnienie obowiązków związanych z okresami przechowywania dokumentacji pracowniczej nie oznacza jednak automatycznie spełnienia wymagań z przepisów o ochronie danych osobowych. Aby to zobrazować, posłużmy się przykładem: spółka przechowuje akta osobowe byłych pracowników w archiwum działu personalnego, a wśród tych akt znajdują się akta, co do których obowiązek ich przechowywania przez okres 50 lat zakończył się w 2018 r. W ocenie spółki z uwagi na to, że akta te znajdują się w archiwum, zrealizowała ona przepisy o ochronie danych osobowych i nie jest zobowiązana do podjęcia żadnych czynności. Postępowanie to jest nieprawidłowe, ponieważ spółka po upływie okresu przetwarzania danych (50 lat) nie usunęła danych osobowych. Akta osobowe po upływie okresu ich przechowywania powinny ulec trwałemu zniszczeniu. Fakt, że znajdują się one w archiwum działu personalnego oznacza, że administrator nadal posiada do nich dostęp, zatem dane osobowe zawarte w aktach – w rozumieniu RODO – nadal są przetwarzane.

## III. ZMIANY W PRZEPISACH DOTYCZĄCYCH ZFFŚ

Na podstawie ustawy wdrożeniowej zostaną także wprowadzone zmiany w ustawie z 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (t.j. Dz.U. z 2018 r. poz.

1316 ze zm.) – dalej jako: **ustawa o ZFŚS**. Potrzeba ich wprowadzenia wynikła stąd, że przepisy prawa pracy nakładają na pracodawcę obowiązek sprawowania funkcji społecznych w stosunku do najbardziej potrzebujących rodzin pracowników, a w celu jego realizacji przetwarza on dane osobowe nie tylko pracowników, ale również członków ich rodzin.

Po wejściu w życie RODO pojawiły się wątpliwości przy stosowaniu obecnych przepisów dotyczących ZFŚŚ. Dotyczyły one w szczególności:

1) zakresu gromadzonych danych osobowych (tj. jakie dane osobowe pracodawca mógł zbierać od pracowników i członków ich rodzin),

2) sposobu zabezpieczenia tych danych,

3) okresu przechowywania danych oraz

4) sposobu wypełnienia obowiązku informacyjnego.

Dostosowując poszczególne przepisy prawa pracy do RODO w ustawie wdrożeniowej dokonano także nowelizacji ustawy o ZFŚS. Jednakże wprowadzane właśnie zmiany nie rozwiążą w całości wskazanych powyżej wątpliwości. Nowelizacja dotyczy bowiem wyłącznie kwestii, które są związane z bezpieczeństwem przetwarzanych danych osobowych. Powyższa materia, zdaniem ustawodawcy, zasługiwała na specjalną ochronę prawną, albowiem pracownicy uprawnieni do świadczeń z funduszu przekazują w związku z tym dane osobowe szczególnej kategorii (np. dane o sytuacji zdrowotnej pracownika lub członków jego rodziny).

**Na podstawie oświadczenia**

Pierwsza zmiana dotyczy formy przekazywania danych osobowych na potrzeby skorzystania przez pracownika ze świadczeń ZFŚS. Od 4 maja udostępnienie pracodawcy danych ma następować w formie oświadczenia, przy czym ustawodawca nie wskazał wzoru tego oświadczenia. Oczywiście pracownik może samodzielnie takie oświadczenie sporządzić, jednak w wielu firmach, w szczególności zatrudniających kilkuset lub więcej pracowników, działy personalne już teraz korzystają ze wzorów wniosków o przyznanie świadczenia z funduszu. Po wejściu w życie nowych przepisów, konieczne będzie zatem zweryfikowanie dotychczasowych wzorów wniosków oraz nadanie im formy oświadczenia. Takie oświadczenie będzie poczytywane jako zgoda pracownika na przetwarzanie jego danych osobowych (podstawę prawną stanowi art. 6 ust. 1 lit. a RODO, natomiast w zakresie danych szczególnej kategorii – art. 9 ust. 2 lit. a i b RODO).

**Dostęp do informacji o zdrowiu**

Po zmianach, które wprowadzi ustawa wprowadzająca RODO, przyznanie pracownikom dostępu do danych osobowych innych pracowników dotyczących zdrowia, a przetwarzanych w ramach ZFŚS, będzie mogło mieć miejsce wyłącznie na podstawie indywidualnego, pisemnego upoważnienia wystawionego przez pracodawcę. Bez wątpienia wpłynie to na zapewnienie odpowiedniego poziomu poufności dla

przetwarzania tego typu informacji, co ma znaczenie w szczególności z uwagi na to, że przetwarzane dane niejednokrotnie dotyczą zarówno sytuacji zdrowotnej, jak i finansowej. Aby właściwie nadać upoważnienia, pracodawca powinien uprzednio zidentyfikować zbiory danych osobowych, jakie są przetwarzane w organizacji. Jeżeli u pracodawcy w ramach takich zidentyfikowanych zbiorów funkcjonuje ZFŚS, to dane osobowe przetwarzane w ramach funduszu będą stanowiły zapewne odrębny zbiór danych. Po zidentyfikowaniu rodzaju danych oraz miejsc przetwarzania należy zweryfikować, jaki krąg osób ma do nich dostęp w ramach zbioru ZFŚS oraz w jakiej formie (pisemnej, elektronicznej – przy czym ta pierwsza jest rekomendowana ze względu na cele dowodowe). Po uzyskaniu tych informacji możliwe będzie właściwe nadanie upoważnień (patrz przykład 6). Zaleca się przy tym, aby pracodawca prowadził rejestr upoważnień, w którym określi do jakich danych poszczególne osoby mają dostęp – takie rozwiązanie z pewnością korzystnie wpłynie na dookreślenie zakresu dostępu do danych, co jest również ważne przy dokonywaniu wymaganej przepisami RODO analizy ryzyka.

**Przykład 6**

**Upoważnienia i ograniczenia**

Po dokonaniu identyfikacji zbiorów i zakresu przetwarzanych danych osobowych w ramach ZFŚS pracodawca postanowił nadać trzem pracownikom działu personalnego pisemne upoważnienia do przetwarzania danych osobowych w ramach funduszu. Jednocześnie z uwagi na to, że dostęp do danych ZFŚS będą miały tylko trzy osoby, pracodawca dokonał weryfikacji kręgu osób mających dostęp do systemu, w którym są przetwarzane dane gromadzone na potrzeby tego funduszu, oraz katalogu na dysku sieciowym, w którym zapisane są skany dokumentacji ZFŚS. Pracodawca ograniczył dostęp do ww. danych zapisanych w systemie oraz w katalogu na dysku sieciowym wszystkim innym osobom, poza pisemnie upoważnionymi pracownikami.

Należy również pamiętać, że dostęp do danych osobowych przetwarzanych w ramach ZFŚŚ posiadają nie tylko pracownicy działu personalnego, lecz również członkowie komisji socjalnych. Pracodawca powinien w związku z tym rozważyć nadawanie im czasowych upoważnień do przetwarzania danych osobowych.

## Co gromadzić na potrzeby funduszu

Zmiany, które wprowadzi ustawa wdrożeniowa, nie dotyczą natomiast wskazania, jakie konkretnie dane osobowe pracowników oraz członków ich rodzin będą mogły być przez pracodawcę przetwarzane. Nowelizacja przewiduje jedynie, że pracodawca może żądać udokumentowania danych osobowych w zakresie niezbędnym do ich potwierdzenia. Takie potwierdzenie może odbywać się w szczególności na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej), rodzinnej i materialnej osoby uprawnionej do korzystania z funduszu. Jakich zatem dokumentów i jakich danych

osobowych może zażądać pracodawca? Z pewnością są to informacje dotyczące sytuacji rodzinnej i majątkowej (przekazywane w formie oświadczenia lub – w niezbędnym zakresie, jeżeli wymagane jest potwierdzenie przekazywanych danych – również zaświadczenia), dokumentacja medyczna itd.

**Jak długo przechowywać dokumentację**

Z uwagi na wprowadzoną przez RODO zasadę ograniczoności przetwarzania danych, polski ustawodawca wprowadził zapis, że przetwarzanie może odbywać się przez okres niezbędny do przyznania ulgowej usługi i świadczenia, dopłaty z funduszu oraz ustalenia ich wysokości, a także przez okres niezbędny do dochodzenia praw lub roszczeń. Dane osobowe przetwarzane w związku z udzielaniem świadczeń z funduszu mogą być poddawane kontroli przez Zakład Ubezpieczeń Społecznych, urząd skarbowy czy inne organy. Z uwagi na przedawnienie roszczeń publicznoprawnych, które wynosi pięć lat, dane osobowe przetwarzane w ramach ZFŚS powinny być przetwarzane nie dłużej, niż przez ten okres. Przy czym dotyczy to tych danych, które są istotne w celu wykazania prawidłowości przyznanego świadczenia. Dodatkowo ustawa wdrożeniowa nałożyła na pracodawców obowiązek dokonywania – nie rzadziej niż raz w roku kalendarzowym – przeglądu danych osobowych przetwarzanych w związku z realizacją świadczeń z ZFŚS w celu ustalenia niezbędności ich dalszego przechowywania. W przypadku stwierdzenia, że przetwarzanie tych danych nie jest już niezbędne, konieczne będzie ich usunięcie lub trwałe zanonimizowanie (dotyczy to dokumentacji papierowej, systemów elektronicznych oraz jakichkolwiek nośników danych).

**Dane członków rodziny**

Jak już wskazano powyżej, podstawę przetwarzania danych pracownika w związku z ubieganiem się przez niego o świadczenia z funduszu stanowi oświadczenie, zawierające zgodę na przetwarzanie danych osobowych. Często jednak w związku z realizacją zadań z ZFŚŚ, pracodawcy przetwarzają dane osobowe członków rodzin pracowników, które nierzadko stanowią dane szczególnej kategorii. W jaki sposób legalnie pozyskać i przetwarzać takie dane wrażliwe w celu realizacji świadczeń z funduszu? Niestety znowelizowane przepisy – a także uzasadnienie do ustawy – w żaden sposób wprost nie odnoszą się do tej sytuacji. Podstawy przetwarzania tych danych należy zatem szukać w art. 9 ust. 2 RODO, który to wskazuje podstawy przetwarzania danych wrażliwych.

**Poinformowanie o zasadach przetwarzania**

Jakie dodatkowe czynności powinien podjąć pracodawca, aby dostosować, sposób przetwarzania danych w związku z udzielaniem świadczeń z ZFŚS do przepisów o ochronie danych osobowych? Oprócz opisanych już wyżej modyfikacji wzorów wniosków w celu wprowadzenia oświadczeń oraz nadania pracownikom odpowiednich upoważnień konieczne będzie:

1. dokonanie przeglądu „starej” dokumentacji pod względem upływu okresu przechowywania danych,
2. wprowadzenie zmian do treści obowiązku informacyjnego w zakresie przetwarzania danych osobowych w związku z realizacją świadczeń z ZFŚS – dotyczy to wszystkich osób, których dane osobowe są przetwarzane w ramach ZFŚS – również członków rodzin,
3. odpowiednie zabezpieczenie nośników danych osobowych, na których są przetwarzane dane zwłaszcza zawierające dane szczególnej kategorii (np. na temat zdrowia),
4. dostosowanie postanowień regulaminu określającego zasady i warunki korzystania z usług i świadczeń finansowanych z funduszu.

## SYSTEMY WYKORZYSTYWANE PRZEZ PRACODAWCĘ

Coraz więcej procesów przetwarzania danych osobowych pracowników odbywa się z wykorzystaniem systemów informatycznych. Ma to z pewnością na celu ułatwienie organizacji procesu pracy. Korzystanie z takich systemów przez administratora danych oznacza jednak, że muszą one nie tylko posiadać odpowiednie parametry techniczne, ale także być dostosowane do obowiązujących przepisów o ochronie danych osobowych. Odpowiedzialność za korzystanie z nośników danych – czyli również z systemów, programów czy aplikacji – spoczywa na administratorze danych, którym w zakresie przetwarzania danych pracowników jest pracodawca. Zatem to pracodawca, jako administrator tych danych, a nie dostawca systemu będzie ewentualnie pociągnięty do odpowiedzialności za przetwarzanie danych osobowych niezgodnie z RODO i to na niego może zostać nałożona kara przez UODO. Co więcej, fakt, że dostawca systemu nie dostosował go do RODO nie powoduje, że pracodawca korzystający z takiego systemu będzie zwolniony z odpowiedzialności. To na administratorze ciąży bowiem obowiązek korzystania z takich narzędzi, które będą posiadały nie tylko odpowiednie zabezpieczenia, lecz również funkcjonalności wymagane przez RODO.
Powyższe rozważania odnoszą się także do kandydatów na pracowników. Firmy coraz częściej korzystają bowiem również z systemów do przetwarzania danych osobowych kandydatów pozyskanych w procesie rekrutacji. Również i w tym przypadku należy zadbać o to, aby były one zgodne z RODO, tj. posiadały odpowiednie funkcjonalności. W procesie rekrutacji istotne jest m.in. terminowe usunięcie danych osobowych kandydatów, którzy nie zostali zatrudnieni w związku z prowadzonym procesem rekrutacji, zatem system powinien mieć odpowiednią funkcję usunięcia danych. W przeciwnym razie po upływie okresu przetwarzania danych – który powinien być określony w obowiązku informacyjnym – pracodawca będzie przetwarzać dane osobowe bez podstawy prawnej.

### Digitalizacja dokumentacji pracowniczej

W kontekście przetwarzania danych w systemach elektronicznych pracodawca powinien uwzględnić również to, że od 1 stycznia 2019 r. istnieje możliwość prowadzenia akt pracowniczych także w formie cyfrowej. Zmiany kodeksu pracy w tym zakresie mają docelowo przyspieszyć proces opracowania dokumentów, skrócić czas przeszukiwania akt pracowniczych, a także poprawić jakość prowadzanej dokumentacji. Wybór formy prowadzenia akt pracowniczych – papierowej lub elektronicznej – należy do pracodawcy, a postać cyfrowa jest równoważna papierowej.

Rozporządzenie w sprawie dokumentacji pracowniczej określa przy tym środki, jakie należy wdrożyć w przypadku prowadzenia dokumentacji pracowniczej w postaci elektronicznej:

a. zabezpieczenie przed uszkodzeniem, utratą oraz nieuprawnionym dostępem;
b. integralność treści dokumentacji i metadanych polegająca na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem tych dokonywanych w ramach ustalonych i udokumentowanych procedur;
c. stały dostęp do dokumentacji osobom do tego upoważnionym;
d. identyfikacja osób mających dostęp do dokumentacji oraz rejestrowanie dokonywanych przez te osoby zmian w dokumentacji i metadanych;
e. skuteczne wyszukiwanie dokumentacji na podstawie określonych metadanych,
f. wydawanie, w tym przez eksport w postaci elektronicznej, dokumentacji albo części dokumentacji w przewidziany przepisami sposób;
g. funkcjonalność wydruku dokumentacji.

**Co trzeba zmienić dotychczasowych rozwiązaniach**

Z uwagi na korzystanie z systemów informatycznych, niezbędne jest zweryfikowanie przez pracodawców tych systemów w zakresie posiadanych funkcjonalności, możliwości realizacji praw osób, których dane są w tych systemach przetwarzane, a także posiadanych zabezpieczeń. System powinien posiadać możliwość – w zależności od podstaw przetwarzania danych osobowych – realizacji praw określonych w RODO np. prawa do bycia zapomnianym czy prawa do przenoszenia danych. Brak ich realizacji oznaczać będzie niewypełnienie przepisów RODO poprzez wykorzystywanie narzędzia, które nie jest dostosowane do przepisów. Przy projektowaniu systemów i ich wdrażaniu – jeżeli są w nich przetwarzane dane osobowe – konieczne jest stworzenie i posiadanie dokumentacji dotyczącej systemów, która w przypadku ewentualnej kontroli będzie stanowiła przedmiot zainteresowania organu nadzoru.
RODO nakłada na administratora – czyli na pracodawcę – również obowiązek dokonania oceny ryzyka naruszenia praw lub wolności pracownika oraz wdrożenia odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych, np. poprzez pseudonimizację i szyfrowanie danych osobowych. Pracodawca musi również zapewnić, aby system był zdolny do:

1) ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

2) szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Obowiązkiem pracodawcy jest również regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych przez niego środków technicznych i organizacyjnych. W przeciwnym przypadku za korzystanie z systemu, który jest niezgodny z RODO, administrator będzie mógł zostać pociągnięty do odpowiedzialności.

## EKSPERT RADZI: JAK PRZETWARZAĆ DANE PRACOWNIKÓW ZGODNIE Z RODO

Przetwarzanie danych osobowych przez pracodawcę, pomimo dostosowania przepisów krajowych do RODO na skutek nowelizacji przepisów prawa pracy, w dalszym ciągu może stanowić spore wyzwanie pod kątem prawidłowości realizacji zasad ochrony danych osobowych. Przepisy często są bowiem nieostre, a nadal nie ma wypracowanej praktyki w zakresie ich właściwej interpretacji. Zauważyć można również, że polskie organy, które są podmiotami upoważnionymi do dokonywania wykładni tj. Ministerstwo Cyfryzacji czy UODO, często przedstawiają zupełnie odmienne opinie na temat rozumienia tych samych przepisów, co z pewnością nie wpływa pozytywnie na postępowanie przedsiębiorców. Tymczasem kontrola może być przeprowadzona u każdego pracodawcy, a sankcje mogą dotyczyć nie tylko przypadków wycieku danych, ale również niewypełnienia formalizmów wynikających z przepisów o ochronie danych osobowych (np. braku wdrożonych procedur czy dokumentacji). Z tego względu poniżej zaprezentowano zestawienie przykładowych działań, jakie powinien podjąć pracodawca, aby sprostać wymaganiom nałożonym przez ustawodawcę.

1. **Proces rekrutacji**

    - zbieranie tylko takiego zakresu danych, jakie jest dozwolone na podstawie obowiązujących przepisów,
    - każdorazowe zbieranie zgód na przetwarzanie danych osobowych kandydatów do pracy, z rozróżnieniem aktualnego procesu rekrutacji i przyszłego,
    - wypełnienie względem kandydata obowiązku informacyjnego,
    - realizacja zasady rozliczalności poprzez udowodnienie, że kandydat wyraził zgodę na przetwarzanie jego danych osobowych oraz że zapoznał (lub miał możliwość) zapoznania się z obowiązkiem informacyjnym,
    - nadanie pracownikom prowadzącym proces rekrutacji upoważnienia w tym zakresie oraz zobowiązanie ich do zachowania poufności,
    - usuwanie dokumentów i danych kandydatów po upływie okresu ich przetwarzania (dotyczy to również korespondencji mailowej, a także wszelkich danych zapisanych w formie papierowej czy elektronicznej),

- jeżeli dane osobowe kandydatów są powierzane przez pracodawcę innym podmiotom (np. podmiotom świadczącym usługę utrzymania programu, w którym są przetwarzane te dane) należy zawrzeć z takimi podmiotami umowę powierzenia przetwarzania danych.

**2. Przetwarzanie danych pracowników**

- zbieranie danych w takim zakresie, jaki jest określony w obowiązujących przepisach, w szczególności w kodeksie pracy,
- wypełnienie obowiązku informacyjnego wobec pracowników z uwzględnieniem wszystkich podstaw przetwarzania danych,
- realizacja zasady rozliczalności poprzez udowodnienie, że pracownik zapoznał (lub miał możliwość) zapoznania się z obowiązkiem informacyjnym,
- w przypadku przetwarzania danych pracowników na podstawie zgody (np. wizerunek) zebranie zgody oraz udowodnienie, że pracownik tej zgody udzielił,
- jeżeli na terenie zakładu pracy zainstalowano monitoring, informację w tym zakresie należy zamieścić w obowiązku informacyjnym, regulaminie pracy oraz ewentualnie w innych aktach wewnętrznych pracodawcy; obszar monitoringu należy oznaczyć poprzez umieszczenie znaków graficznych i wywieszenie tablicy zawierającej obowiązek informacyjny; konieczne jest także wypełnienie przepisów k.p. w zakresie dostosowania celów i okresu przetwarzania danych z monitoringu,
- nadanie pracownikom upoważnienia do przetwarzania danych osobowych pracowników oraz zobowiązanie ich do zachowania poufności,
- prowadzenie archiwum akt osobowych zgodnie z okresem ich przechowywania wskazanym w przepisach (aktualnie 10 lub 50 lat),
- jeżeli dane osobowe pracowników są przekazywane podmiotom zewnętrznym (np. biurom rachunkowym) konieczne jest zawarcie z tymi podmiotami umowy powierzenia przetwarzania danych,
- w przypadku przetwarzana danych biometrycznych należy uzyskać zgodę pracownika oraz wypełnić przesłanki określone w kodeksie pracy w zakresie możliwości stosowania kontroli dostępu do wybranych pomieszczeń pracodawcy,
- w przypadku przetwarzania danych na potrzeby realizacji świadczeń z ZFŚS – dostosowanie oświadczenia pracownika do znowelizowanych przepisów, wypełnienie obowiązku informacyjnego wobec osób, których dane są przetwarzane, przetwarzanie danych z uwzględnieniem zasady minimalizacji danych oraz nadanie upoważnień osobom (w tym członkom komisji socjalnej), które przetwarzają te dane,

- jeżeli pracodawca przetwarza dane z wykorzystaniem systemów IT konieczne jest nie tylko ich odpowiednie zabezpieczenie, lecz również weryfikowanie czy system posiada funkcjonalności zgodne z przepisami o ochronie danych osobowych.

Autorzy:

Anna Hoffmann, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp. k.

Michał Dutkiewicz, prawnik, Kancelaria Prawna Piszcz i Wspólnicy sp. k.