

STOSOWANIE RODO W SPRAWACH PRACOWNICZYCH

1. Zakładowe zasady przetwarzania danych	str. 1	7. Zmiana regulaminów zakładowych pod kątem RODO	str. 3
2. Podstawowe zasady ochrony danych osobowych w świetle RODO	str. 2	8. Zakładowe zasady monitoringu	str. 3
3. Lista obecności zgodnie z nowymi zasadami ochrony danych osobowych	str. 2	9. Uregulowanie tzw. polityki kluczy	str. 3
4. Dokumenty pracownicze z ubiegłych lat a RODO	str. 2	10. Prowadzenie dokumentacji pracowniczej przez biuro rachunkowe	str. 4
5. Aktualność zgody na przetwarzanie danych osobowych	str. 2	11. Upoważnienie pracownika do przetwarzania danych osobowych	str. 4
6. Klauzule informacyjne dla pracowników	str. 3	12. Działalność socjalna a ochrona danych osobowych	str. 4
		13. Ochrona danych w zakładzie pracy chronionej	str. 4

1. Zakładowe zasady przetwarzania danych

Od 25 maja 2018 r. obowiązują przepisy 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... (Dz. Urz. UE L z 2016 r. 119/1), zwanego RODO. Ich uszczegółowienia dokonano ustawą o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 ze zm.). Dostosowanie porządku krajowego do wymogów RODO i powołanej ustawy nastąpi natomiast na podstawie przepisów projektowanej (obecnie w fazie legislacyjnej) ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679.

Jedną z konsekwencji wejścia w życie RODO jest konieczność dostosowania treści obowiązujących w danej firmie przepisów zakładowych do wymogów wynikających z unijnego rozporządzenia. RODO obowiązuje niezależnie od krajowych regulacji dotyczących ochrony danych osobowych. Zapisy regulacji wewnątrzzakładowych (układu zbiorowego pracy, regulaminu pracy i wynagradzania, regulaminu ZFŚS) powinny więc zostać przeanalizowane pod kątem zgodności z zasadami przetwarzania danych wynikającymi z art. 5 RODO (patrz ramka). Wymaga to rozszerzenia w regulaminach zakładowych katalogu obowiązków pracodawcy o wymóg postępowania w zakresie ochrony danych osobowych zgodnie z zasadami RODO i przepisami krajowymi. Konieczne jest też uzupełnienie listy obowiązków pracownika o taki sam wymóg – co ma istotne znaczenie wobec pracowników mających szerszy dostęp do danych osobowych.

Klauzula informacyjna

RODO znacznie rozszerzyło zakres informacji przekazywanych

przez administratora danych (tu pracodawcę) osobom, których dane są przetwarzane. Ma to związek z przyznaniem im szeregu nowych uprawnień, np. prawa do bycia zapomnianym. Informacje o tych uprawnieniach powinny znaleźć się w tzw. klauzulach informacyjnych przekazywanych osobom, od których są pobierane dane, np. od kandydatów do pracy. W przypadku już zatrudnionych pracowników przekazanie wspomnianych klauzul nie jest bezwzględnie obowiązkowe. Niemniej wydaje się to celowe, ponieważ w ten sposób pracownicy zostaną poinformowani o nowych uprawnieniach przysługujących im na mocy RODO.

Przepisy RODO nie określają sposobu przekazania klauzuli informacyjnej pracownikom, można więc ją włączyć do układu zbiorowego bądź regulaminu pracy. Nie jest to jednak wymagane – pracodawca może opracować klauzulę w formie odrębnego dokumentu i zapoznać z nią indywidualnie każdego z pracowników. Wybór formy poinformowania pracowników o przyznanych im przez RODO uprawnieniach należy do pracodawcy.

Sankcje za naruszenie RODO

Za naruszenie regulacji chroniących dane osobowe pracodawcy grożą surowe kary finansowe, określone w art. 83 RODO. Administratorowi za nieprzestrzeganie przepisów RODO grozi kara finansowa, której wartość jest ustalana adekwatnie do okoliczności konkretnego przypadku, z zastrzeżeniem maksymalnej kwoty. Według art. 83 RODO, wysokość kary nie może być wyższa niż:

- 10 mln euro, a dla przedsiębiorstw – 2% całkowitego rocznego światowego obrotu za poprzedni rok obrotowy, lub
- 20 mln euro, a dla przedsiębiorstw – 4% całkowitego rocznego światowego obrotu za poprzedni rok obrotowy.

Stosowne kary przewiduje też art. 101 ustawy o ochronie danych osobowych.

Rejestr czynności przetwarzania

Każdy podmiot przetwarzający dane (m.in. pracodawca) oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego, ma obowiązek prowadzenia rejestru wszystkich kategorii czynności przetwarzania, dokonywanych w imieniu administratora. Rejestry te mają formę pisemną, w tym formę elektroniczną. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego, udostępniają rejestr na żądanie organu nadzorczego. Z obowiązku prowadzenia rejestru czynności przetwarzania danych zwolnieni są tylko przedsiębiorcy lub podmioty zatrudniające mniej niż 250 osób, chyba że przetwarzanie, którego dokonują:

- może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie ma charakteru sporadycznego lub
- obejmuje szczególne kategorie danych osobowych (dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne lub dotyczące zdrowia, seksualności bądź orientacji seksualnej danej osoby) lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Ustawodawca nie wskazał konkretnych technicznych środków zabezpieczenia danych zawartych w dokumentacji papierowej, w tym pracowniczej. Nie określił też wymogów, jakie muszą spełniać szafy, w których akta są przechowywane. Pewne rozwiązania wypracowała natomiast prakty-

ka. Przyjmuje się zatem, że akta osobowe powinny być przechowywane w zamykanych szafach odpowiednio zabezpieczonych, do których dostęp mają tylko wyznaczeni (upoważnieni) pracownicy. Pomieszczenia, w których one stoją powinny być zabezpieczone tak, aby nikt nieupoważniony nie miał do nich dostępu. Nie mogą być narażone na wilgoć czy zalanie, co mogłoby spowodować zniszczenie akt.

Inspektor ochrony danych

Krąg podmiotów zobowiązanych do powołania inspektora danych osobowych w miejsce dotychczasowych administratorów danych osobowych określa art. 37 ust. 1 w związku z motywem 97 preambuły RODO. Są to:

- organy lub podmioty publiczne (z wyjątkiem sądów w zakresie sprawowania wymiaru sprawiedliwości),
 - podmioty, których główna działalność polega na przetwarzaniu danych wymagających regularnego i systematycznego monitorowania osób na dużą skalę z uwagi na swój charakter, zakres lub cel,
 - podmioty zajmujące się przede wszystkim przetwarzaniem na dużą skalę danych wrażliwych, w tym związanych ze stanem zdrowia (art. 9 ust. 1 RODO).
- W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności.

Podstawowe zasady przetwarzania danych zgodnie z RODO

Przetwarzanie danych osobowych przez pracodawców powinno uwzględniać zasady tego przetwarzania, określone m.in. w art. 5 RODO. Zgodnie z tym przepisem dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości),
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, z zastrzeżeniem możliwości dalszego przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych albo do celów statystycznych (zasada ograniczenia celu),
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych),
- prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości),
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane; dane osobowe można przechowywać przez okres dłuższy tylko przy spełnieniu określonych warunków (zasada ograniczenia przechowywania),
- 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 (zasada integralności i poufności).

2. Podstawowe zasady ochrony danych osobowych w świetle RODO

Zasada	Wytyczne co do stosowania	Uwagi
zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO)	pracownik musi wiedzieć przez kogo, w jakim celu i na jakiej podstawie prawnej jego dane osobowe są zbierane, wykorzystywane lub w inny sposób przetwarzane, a informacje związane z przetwarzaniem (w tym prawa pracownika) mają być dla niego łatwo dostępne, zrozumiałe oraz sformułowane jasnym i przystępnym językiem (motyw 39–47, 58 i 60 preambuły RODO)	realizacja tej zasady wymaga: – podania przesłanek legalności przetwarzania, wskazanych w art. 6 i 9 RODO, – spełnienia obowiązków informacyjnych, o jakich mowa w art. 13–14 RODO
ograniczenia celu (art. 5 ust. 1 lit. b RODO)	– dane osobowe mają być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych albo do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami (motywy 39 i 50 preambuły RODO), – pracownik ma uzyskać informację o celach w momencie zbierania danych albo później, jeśli pracodawca będzie chciał przetwarzać dane w innych celach (motyw 61 preambuły RODO)	– w przypadku stosunków pracy, cele ograniczają się do wykonywania praw i obowiązków z nich wynikających, – cel przetwarzania danych pracodawca zamieszcza w klauzulach informacyjnych, przygotowywanych zgodnie z art. 13–14 RODO
minimalizacji danych (art. 5 ust. 1 lit. c RODO)	dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane (motyw 39 preambuły RODO)	pracodawca powinien selekcjonować dane osobowe i wybierać tylko te, które są niezbędne do realizacji celu (celów), w których zostały zebrane
prawidłowości (art. 5 ust. 1 lit. d RODO)	dane osobowe mają być prawidłowe i w razie potrzeby uaktualniane, a nieprawidłowe – niezwłocznie prostowane lub usuwane (motyw 39 i 65 preambuły RODO)	prawo do sprostowania nieprawidłowych danych oraz ich usunięcia przysługuje pracownikowi na podstawie art. 16–17 RODO
ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO)	– okres przechowywania danych powinien być zredukowany do ścisłego minimum, adekwatnego do celu ich przetwarzania, a jego przekroczenie może być uzasadnione jedynie celami archiwalnymi, naukowymi, historycznymi i statystycznymi, – aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, pracodawca powinien ustalić termin ich usuwania lub okresowego przeglądu (motyw 39 preambuły RODO)	– okres przechowywania dokumentacji pracowniczej jest określony obecnie na podstawie przepisów o archiwach i emeryturach i wynosi zasadniczo 50 lat; od 1 stycznia 2019 r. zostanie skrócony do 10 lat w stosunku do pracowników zatrudnionych począwszy od tego dnia; wskazany termin będzie też dotyczył pracowników zatrudnionych po dniu 31 grudnia 1998 r. a przed dniem 1 stycznia 2019 r., oraz pozostających w zatrudnieniu, jeśli pracodawca złoży za nich raport informacyjny do ZUS; 10-letni termin nie będzie dotyczył pracowników zatrudnionych przed 1 stycznia 1999 r., – okres przechowywania danych powinien być wskazany w klauzuli informacyjnej przekazywanej pracownikowi, zgodnie z art. 13–14 RODO
integralności i poufności (art. 5 ust. 1 lit. f RODO)	dane mają być przetwarzane w sposób zapewniający im bezpieczeństwo, ochronę przed niedozwolonym i niezgodnym z prawem przetwarzaniem, utratą, zniszczeniem lub uszkodzeniem, przy użyciu odpowiednich środków technicznych i organizacyjnych (motyw 39 preambuły RODO)	– dostęp do danych mają mieć wyłącznie osoby upoważnione przez pracodawcę (art. 29 RODO), – wszystkie osoby mające dostęp do danych są zobowiązane do zachowania ich w tajemnicy (m.in. art. 9 ust. 3 RODO)
rozliczalności (art. 5 ust. 2 RODO)	pracodawca ma obowiązek wykazać, że postępuje zgodnie z zasadami RODO	– pracodawca musi być w stanie udowodnić, że jego działania są zgodne ze wszystkimi opisanymi wyżej regułami, – jeśli pracodawca pozyskuje zgody pracowników na przetwarzanie danych, musi wykazać, że spełniają one warunki art. 7 RODO i innych jego regulacji

3. Lista obecności zgodnie z nowymi zasadami ochrony danych osobowych

W naszym zakładzie stosowana jest lista obecności, na której pracownicy zaznaczają nieobecności używając symboli literowych, np. choroba (Ch), wyjście prywatne (Pr) czy urlop (Uw). Czy po wejściu w życie RODO jest to prawidłowa praktyka?

NIE. Od 25 maja 2018 r., tj. od dnia wejścia w życie rozporządzenia RODO, przetwarzanie danych osobowych pracownika musi mieć konkretną podstawę prawną i cel. Istotny jest zwłaszcza cel przetwarzania danych osobowych. Zgodnie z art. 5 ust. 1 lit. b) oraz motywem 39 preambuły RODO powinien on być konkretny, wyraźny i prawnie uzasadniony.

Przetwarzanie danych jest zgodne z przepisami (krajowymi oraz RODO), jeżeli m.in.:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- przetwarzanie jest niezbędne do wypełnienia obowiązku

prawnego ciążącego na administratorze.

Przesłanki te wynikają z art. 6 ust. 1 RODO. Nie można jednak stwierdzić, że występują w przedstawionej sytuacji. Lista obecności służy do weryfikacji obecności lub nieobecności w pracy danego pracownika. Dla realizacji tego celu wystarczające jest potwierdzenie obecności w pracy podpisem (parafką) pracownika, a nieobecności przez symbol N lub postawienie kreski. Ujawnianie przyczyny absencji pracownika w liście obecności nie jest też konieczne dla realizacji uprawnień bądź obowiązków wynikających z umowy o pracę ani do wypełnienia obowiązku ciążącego na administratorze danych (tu: pracodawcy). Ponadto jest mało prawdopodobne, że pracownik wyraził zgodę na udostępnienie danych dotyczących przyczyny jego absencji wszystkim osobom, które mają lub potencjalnie mogą mieć dostęp do

listy obecności (która zazwyczaj znajduje się w ogólnie dostępnym miejscu). Zaznaczenie na niej przyczyny nieobecności nie będzie więc miało podstaw w obecnie obowiązujących przepisach dotyczących ochrony danych osobowych.

Adnotacja o chorobie w liście obecności może zostać uznana za naruszenie RODO, które zabrania przetwarzania danych wrażliwych, jakimi są informacje o zdrowiu.

Oznaczenie przyczyny nieobecności określonymi symbolami może zostać uznane za niezgodne z wynikającą z art. 5 ust. 1 lit. b) oraz motywu 50 preambuły RODO zasadą ograniczenia celu przetwarzania danych. Może również prowadzić do naruszenia zasady poufności danych (art. 5 ust. 1 lit. f RODO), z którą związany jest wymóg dopuszczenia do przetwarzania danych osobowych tylko tych osób, które posiadają odpowiednie upoważnienie.

4. Dokumenty pracownicze z ubiegłych lat a RODO

W aktach osobowych pracownika przechowujemy kserokopie świadectw pracy dotyczących poprzedniego zatrudnienia, świadectw szkolnych i innych dokumentów potwierdzających np. kwalifikacje zawodowe pracownika. Zawierają one zakres danych szerszy niż obecnie można uzyskiwać. Co zrobić z takimi dokumentami, czy nadal mogą być w aktach osobowych?

Pracodawca ma prawo przechowywać w aktach osobowych pracownika kopie świadectw pracy, świadectw szkolnych czy dokumentów potwierdzających kwalifikacje pracownika. Podstawą takiego rozstrzygnięcia są przepisy krajowe w związku z art. 88 RODO.

Pracodawca pozyskuje, a następnie przechowuje dane osobowe pracownika niezbędne do realizacji zawartego z nim stosunku pracy. Zostały one określone w przepisach Kodeksu pracy oraz rozporządzeniu Ministra Pracy i Polityki Socjalnej w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy... (Dz. U. z 2017 r. poz. 894). Na przestrzeni lat przepisy te ulegały zmianie ograniczając zakres danych, których może żądać pra-

codawca. Pojawiło się w związku z tym pytanie, czy dopuszczalne jest przechowywanie w aktach osobowych danych pracownika, pozyskanych w zgodzie z przepisami obowiązującymi w okresie ich pozyskiwania, do przetwarzania których pracodawca nie jest już upoważniony. Ministerstwo Rodziny, Pracy i Polityki Społecznej w odpowiedzi na zapytanie naszego Wydawnictwa uznało, że jest to możliwe (patrz ramka). Analogicz-

ne stanowisko w tej sprawie zajął Główny Inspektor Ochrony Danych Osobowych (GIODO) w piśmie otrzymanym przez Wydawnictwo 16 lipca 2015 r., rozstrzygającym omawianą kwestię w poprzednim stanie prawnym. Jak zauważył GIODO w przywołanej opinii: „(...) dane te mają charakter archiwalny i takie powinny pozostać, jako dokumentujące spełnienie przez pracodawcę jego ustawowych obowiązków”.

„(...) Zdaniem MRPiPS takie dane osobowe nie muszą być usuwane z akt osobowych pracownika wchodzących w skład dokumentacji pracowniczej, jeżeli zostały one pozyskane zgodnie z przepisami obowiązującymi w okresie ich pozyskiwania. Taki sam pogląd prezentują przedstawiciele Urzędu Ochrony Danych Osobowych podczas prac legislacyjnych prowadzonych nad projektem ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679”.

Odpowiedź MRPiPS z dnia 25 czerwca 2018 r. na pytanie naszego Wydawnictwa

5. Aktualność zgody na przetwarzanie danych osobowych

W niektórych przypadkach nasi pracownicy składali oświadczenie o wyrażeniu zgody na przetwarzanie ich danych osobowych (najczęściej na etapie rekrutacji i czasami w trakcie zatrudnienia). Czy te zgody po wejściu w życie RODO są nadal aktualne?

Główny Inspektor Ochrony Danych Osobowych (od 25 maja br. Prezes Urzędu Ochrony Danych Osobowych) na stronie internetowej www.giodo.gov.pl poinformował, że większość zgód pozyskanych pod rządami poprzednich przepisów (tj. do 24 maja 2018 r.) zachowuje ważność, o ile pracownicy uzyskali informację o prawie wycofania zgody w dowolnym momencie (co powinno być dla pracownika tak samo łatwe jak jej wyrażenie). Zgodnie z art. 4 pkt 11 RODO zgoda pracownika na przetwarzanie jego danych osobowych powinna być:

- dobrowolna – pracownik ma

- rzeczywisty i wolny wybór przy udzielaniu zgody, ma prawo odmówić jej udzielenia i wycofania w dowolnym czasie bez niekorzystnych konsekwencji,
- konkretna – treść powinna być dokładnie określona, precyzyjna i rzeczowa; ma odnosić się do celu (np. uzyskania dofinansowania w ramach programu unijnego), w którym dane osobowe będą/są przetwarzane,
- świadoma – pracownik jest świadomy kogo, w jakim celu i w jakim zakresie uprawnia do przetwarzania swoich danych osobowych,
- jednoznaczna – wyrażająca

wolę pracownika w formie oświadczenia (pisemnego, elektronicznego lub ustnego) albo działania potwierdzającego (np. zaznaczenie okienka w danym formularzu), w sposób niebudzący żadnych wątpliwości, że to ten konkretny pracownik dał pracodawcy prawo przetwarzania swoich danych w znanym mu i uprawnionym celu.

W omawianym przypadku pracodawca powinien sprawdzić, czy posiadane zgody są adekwatne do zasad wskazanych w art. 4 pkt 11 RODO i ewentualnie je zaktualizować.

6. Klauzule informacyjne dla pracowników

Musimy przygotować klauzule informacyjne dla pracowników, informujące o tym, że przetwarzamy ich dane dla celów pracowniczych. Jak powinny wyglądać takie klauzule? W jaki sposób przekazywać je pracownikom i gdzie je przechowywać?

Pracownik, którego dane dotyczą, musi być poinformowany o prowadzeniu operacji przetwarzania tych danych i o jej celach. Administrator danych (tu: pracodawca) powinien podać mu wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. W przypadku gdy dane osobowe zbierane są bezpośrednio od danej osoby, administrator danych ma

obowiązek podać tej osobie informacje określone w art. 13 RODO. Obejmują one m.in.:

- tożsamość i dane kontaktowe administratora danych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe jego przedstawiciela,
- dane kontaktowe inspektora ochrony danych (jeżeli zostanie powołany w jednostce),
- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,

- prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO,
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.

Informacje te powinny znaleźć się w tzw. klauzulach informacyjnych przekazywanych osobom, od których dane będą pobierane np. w procesie rekrutacyjnym (patrz: Przykład klauzuli...).

Jeśli chodzi o zatrudnionych już pracowników, to zdaniem redakcji, warto przedstawić im klauzule informacyjne, gdyż chodzi o poinformowanie ich o przysługujących im nowych uprawnieniach wynikających z RODO oraz ustawy o ochronie danych osobowych.

Klauzulę można zamieścić w stopce pracowniczego kwestionariusza osobowego lub np. w stopce formularza oświadczenia o poufności przekazywanego pracownikom do podpisu. Klauzula informacyjna może być też odrębnym dokumentem przekazywanym np. pocztą elektroniczną czy w tradycyjnej wersji papierowej. Po zapoznaniu się pracownika z klauzulą może ona zostać wpięta do jego akt osobowych lub zamieszczona w osobnej dokumentacji utworzonej dla celów związanych z ochroną danych osobowych w zakładzie pracy.

Przykład klauzuli informacyjnej przekazywanej pracownikom

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

- administratorem Pani/Pana danych osobowych jest (nazwa Administratora) z siedzibą w (adres Administratora),
- kontakt z Inspektorem Ochrony Danych – (numer telefonu, e-mail),
- Pani/Pana dane osobowe będą przetwarzane w celu realizacji zatrudnienia w ramach stosunku pracy i przyznawania świadczeń socjalnych – na podstawie art. 6 ust. 1 lit. a), c) ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r., Kodeksu pracy oraz ustawy o zakładowym funduszu świadczeń socjalnych,
- odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa,
- Pani/Pana dane osobowe przechowywane będą przez okres 50 lat,
- posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do cofnięcia zgody,
- przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
- podanie danych osobowych w tym zakresie jest obowiązkiem wynikającym z przepisów prawa.

7. Zmiana regulaminów zakładowych pod kątem RODO

W naszym zakładzie posiadamy regulamin pracy i wynagradzania. Czy w związku z obowiązaniem RODO należy uzupełnić ich treść o zapisy o ochronie danych osobowych (do tej pory w regulaminach ich nie było)?

TAK. Jedną z konsekwencji wejścia w życie RODO jest konieczność dostosowania treści obowiązujących w danej firmie przepisów zakładowych do wymogów wynikających z unijnego rozporządzenia. RODO obowiązuje niezależnie od krajowych regulacji dotyczących ochrony danych osobowych. Przetwarzanie danych osobowych przez

pracodawców powinno uwzględniać zasady tego przetwarzania, określone m.in. w art. 5 RODO (patrz pkt 1 dodatku).

Zapisy regulacji wewnątrzzakładowych (układu zbiorowego pracy, regulaminu pracy i wynagradzania, regulaminu ZFŚS) powinny zostać przeanalizowane pod kątem zgodności z tymi zasa-

dami i odpowiednio skorygowane. Wymaga to rozszerzenia w tych aktach katalogu obowiązków pracodawcy o wymóg postępowania w zakresie ochrony danych osobowych zgodnie z zasadami RODO i przepisami krajowymi (patrz: Przykładowy fragment regulaminu pracy). Konieczne jest też uzupełnienie listy obowiązków pracownika o taki sam wymóg – co ma istotne znaczenie wobec pracowników mających szerszy dostęp do danych osobowych. Do regulaminu pracy lub układu zbiorowego można też wprowadzić treść klauzuli informacyjnej. Wówczas zapoznanie z regulaminem (układem zbiorowym) będzie oznaczało też zapoznanie pracownika z tą klauzulą.

Ponadto, jeżeli pracodawca zamierza wprowadzić do zakładu monitoring wizyjny (albo już go stosuje) powinien uregulować we wspomnianych aktach zakładowych zasady tego monitoringu, uwzględniając regulację RODO.

W regulaminie wynagradzania – w celu dostosowania go do wymogów RODO – należy zamieścić zapisy dotyczące celów przetwarzania danych (którym jest m.in. udokumentowanie prawa do poszczególnych składników wynagrodzenia, ich wysokości i wypłaty), praw przysługujących pracownikowi w zakresie ochrony danych osobowych oraz okresu przechowywania danych.

8. Zakładowe zasady monitoringu

Rozważamy wprowadzenie monitoringu w zakładzie pracy, który będzie polegał na kontroli służbowej poczty, połączeń internetowych i zainstalowaniu kamer w pomieszczeniach przemysłowych i na korytarzach. W jaki sposób uregulować zasady takiego monitoringu – czy wystarczy poinformowanie pracowników o tym, że pracodawca będzie go stosował? Co o monitoringu stanowi RODO?

Monitoring pracownika może przybierać różne formy: nagrywania (tzw. monitoring wizyjny), kontrolowania telefonu i poczty elektronicznej oraz śledzenia połączeń internetowych.

RODO nie zawiera osobnych regulacji dotyczących monitoringu, jednak generalnie (w porównaniu do zasad obowiązujących przed 25 maja 2018 r.) zaostrza zasady przetwarzania danych osobowych i zwiększa zakres informacji, jakie pracownik ma otrzymywać od pracodawcy (art. 13–14 RODO). Z tego powodu zakładowe postanowienia dotyczące tej metody obserwacji powinny być zgodne z określonymi w art. 5 RODO zasadami przetwarzania danych, tj.:

- zgodności z prawem, rzetelności i przejrzystości,
- ograniczenia celu, minimalizacji danych, prawidłowości,
- ograniczenia przechowywania danych, integralności i poufności oraz rozliczalności.

Ustalając procedurę monitoringu, pracodawca powinien dostosować jego zakres i środki do celu, który chce osiągnąć, bez nadmiernej ingerencji w prywatność pracownika. Z tego powodu nie wolno mu monitorować toalet, szatni i stołówek.

Jeżeli podstawą prawną monitoringu nie jest wykonanie obowią-

ku prawnego ciążącego na pracodawcy, lecz jego uzasadniony interes, stosowanie monitoringu wymaga zgody pracownika.

Nagrania obrazu przechowywane przez okres nie dłuższy niż 3 miesiące. Jeżeli jednak stanowią one dowód w postępowaniu prowadzonym na podstawie przepisów prawa lub pracodawca dowiedział się, że mogą one stanowić taki dowód, termin przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

Zasady stosowania monitoringu w danym zakładzie pracy powinny zostać uregulowane w:

- przepisach zakładowych (regulaminie pracy lub układzie zbiorowym), jeżeli pracodawca je posiada lub,
- zarządzeniu wewnętrznym wydanym przez pracodawcę.

W pierwszym przypadku zmiany do regulaminu pracy wejdą w życie po upływie 2 tygodni od podania ich do wiadomości pracowników w sposób zwyczajowo przyjęty w zakładzie pracy. Jeżeli chodzi o zmianę układu zbiorowego, to wchodzi one w życie najwcześniej w dniu rejestracji zmiany (na którą musi się zgodzić druga strona układu jaką jest związek zawodowy) w odpowiednim rejestrze układów.

9. Uregulowanie tzw. polityki kluczy

W naszej firmie niektórzy pracownicy ze względu na charakter ich obowiązków mogli po zakończeniu pracy zabierać klucze od pokoju pracowniczego do domu. Czy aktualnie taka praktyka jest dopuszczalna? Czy zasady postępowania z kluczami do pomieszczeń służbowych powinny być formalnie uregulowane, np. w regulaminie pracy?

Generalnie klucze do pomieszczeń pracowniczych po zakończeniu dnia pracy powinny być zdawane w określonym przez pracodawcę miejscu, np. w portierni bądź sekretariacie danego zakładu pracy. Czasami jednak charakter pracy wykonywanej przez pracownika wymaga, aby niektórzy pracownicy zabierali klucze ze sobą, tak by w każdej chwili mogli wrócić do miejsca pracy. Jest to dopuszczalne, ale w takim przypadku należy te osoby odpowiednio upoważnić do tego, by klucze pozostawiali pod ich osobistym nadzorem. Ponadto należy prowadzić ewidencję osób upoważnionych.

Krajowe przepisy prawa pracy nie zobowiązują pracodawcy do formalnego uregulowania zasad postępowania ze służbowymi kluczami. Podobnie takiego obowiązku nie przewiduje ustawa o ochronie danych osobowych jak też RODO. Jednak jest to wskazane. Opracowana przez pracodawcę polityka kluczy (zamieszczona w przepisach zakładowych lub w osobnym zarządzeniu) będzie jednym z zabezpieczeń w zakresie ochrony danych osobowych i może stanowić część niezbędnej w tym zakresie dokumentacji. Przykładowe zapisy polityki kluczy mogą

przewidywać, że klucze do pomieszczeń są wydawane i zdawane z pomieszczenia portierni/sekretariatu, a klucze zapasowe przechowywane są w portierni (w sekretariacie lub innym miejscu).

W ramach zakładowej polityki kluczy można uregulować kwestie postępowania z kluczami do szafek i biur w pomieszczeniach pracy. Przykładowo można przyjąć zasady, zgodnie z którymi:

- klucze służące do zabezpieczenia biurek i szaf powinny być jednoznacznie opisane,
- w godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie,
- zabronione jest pozostawianie kluczy w biurkach i szafach, w razie nieobecności osób upoważnionych w zakładzie pracy,
- po zakończeniu pracy klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.

Przykładowy druk

Polityka kluczy dostępny jest w serwisie www.druki.gofin.pl, w dziale RODO – Ochrona danych osobowych.

10. Prowadzenie dokumentacji pracowniczej przez biuro rachunkowe

Jesteśmy biurem rachunkowym i świadczymy klientom usługi z zakresu prowadzenia akt osobowych i naliczania wynagrodzeń ich pracowników. Jakie dokumenty oraz urządzenia zabezpieczające musimy posiadać, aby zgodnie z RODO przechowywać teczki akt osobowych pracowników naszych klientów?

Przechowywanie akt osobowych zawierających dane osobowe pracowników jest przetwarzaniem danych osobowych zarówno w rozumieniu krajowych przepisów o ochronie danych, jak i RODO. Administrator danych, czyli pracodawca, może powierzyć przetwarzanie danych innemu podmiotowi w drodze umowy zawartej na piśmie (umowa powierzenia przetwarzania danych). Tak wy-

nika z art. 4 pkt 8 RODO, zgodnie z którym pracodawca może powierzyć przetwarzanie danych innemu podmiotowi, którym może być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Jak wynika z art. 28 ust. 3 RODO, przetwarzanie przez podmiot przetwarzający (np. biuro

podatkowe) jest dopuszczalne wówczas, gdy odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiązą podmiot przetwarzający i administratora. Umowa lub inny akt prawny, wiążący administratora z podmiotem przetwarzającym, powinny mieć formę pisemną, w tym formę elektroniczną (art. 28 ust. 9 RODO).

W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z RODO administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko (motyw 83 preambuły RODO). Obowiązek zastosowania odpowiednich środków technicznych i administracyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane dotyczą, spoczywa na administratorze oraz podmiocie przetwarzającym dane. Możliwe do zastosowania (przykładowe) środki techniczne i organizacyjne wymienia art. 32 ust. 1 RODO, wskazując jako środki zabezpieczenia danych m.in.:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Należy przypomnieć, że osoby wyznaczone w biurze rachunkowym do prowadzenia akt osobowych pracowników zatrudnionych przez danego pracodawcę muszą posiadać stosowne upoważnienie. Upoważnienia mogą wystawić zarówno pracodawca (administrator danych), jak i podmiot przetwarzający (biuro rachunkowe).

11. Upoważnienie pracownika do przetwarzania danych osobowych

Prowadzę jednoosobowo działalność gospodarczą i zamierzam zatrudnić pracownika do prowadzenia spraw kadrowych (do tej pory sam prowadziłem dokumentację swoich pracowników). Czy będę musiał upoważnić nowego pracownika do przetwarzania danych osobowych już zatrudnionych u mnie osób?

TAK. Ustawa o ochronie danych osobowych, w brzmieniu obowiązującym do 24 maja 2018 r., wyraźnie stanowiła, że do przetwarzania danych, czyli m.in. imion, nazwisk, adresów zamieszkania, dat urodzenia, numerów PESEL, danych o rodzinie pracownika,

mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Aktualna ustawa o ochronie danych osobowych nie zawiera regulacji dotyczących upoważnienia do przetwarzania danych osobowych. Nie oznacza to jednak, iż

obecnie takie upoważnienia nie są konieczne. Zasadniczo RODO w żadnym z przepisów nie wspomina bezpośrednio o konieczności pisemnego upoważniania osób mających dostęp do danych osobowych przez administratora danych lub przetwarzającego dane. Jednak w art. 28 stanowi, że jednym z obowiązków administratora danych jest zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Ponadto osoby te mogą przetwarzać dane osobowe tylko na polecenie administratora danych. W związku z tym uznaje się, że nadal konieczne jest upoważnianie m.in. pracowników do przetwarzania danych osobowych.

Upoważnienie nr...2...do przetwarzania danych osobowych

Z dniem...13 listopada 2018 r....upoważniam/anuluje upoważnienie-Panią/Pana*...**Magdalenę Tomańską...**, **pracownicę działu kadr** (imię i nazwisko pracownika, stanowisko, dział)

w zakresie: (WG) wglądu, (W) wprowadzania, (UD) udostępniania, (M) modyfikacji, (A) archiwizacji, (U) usuwania danych osobowych niezbędnych do wypełniania obowiązków pracowniczych. Upoważnienie dotyczy przetwarzania danych osobowych w systemach informatycznych:...**programy kadrowe stosowane w zakładzie**..... (podać nazwy systemów lub programów)

Upoważnienie dotyczy przetwarzania danych osobowych w zbiorach papierowych.....**akta osobowe pracowników**..... (podać nazwy zbiorów)

* niepotrzebne skreślić

12. Działalność socjalna a ochrona danych osobowych

Prowadzimy zakładowy fundusz świadczeń socjalnych.

1) Czy nowe przepisy dotyczące ochrony danych osobowych powodują konieczność zmian w regulaminie zakładowego funduszu świadczeń socjalnych?

TAK. Konieczna jest aktualizacja zapisów regulaminu zakładowego funduszu świadczeń socjalnych w kontekście zasad określonych w art. 5 RODO. To oznacza, iż w regulaminie Funduszu należy wskazać:

- dane podmiotu uprawnionego do zbierania danych osobowych osób uprawnionych do korzystania z zakładowego funduszu świadczeń socjalnych,
- cel przetwarzania danych tych osób, czyli realizację przysługujących im uprawnień z ZFŚS,
- podstawę prawną przetwarzania danych, tj. art. 8 ustawy o zakładowym funduszu świadczeń socjalnych, w związku z art. 6 ust. 1 lit. c) RODO,
- czas przechowywania danych.

Ustawa o ochronie danych osobowych nie zajmuje się zagadnieniem przetwarzania danych dla celów ZFŚS. Czyni to natomiast art. 28 projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (obecnie w toku prac legislacyjnych), nowelizu-

jąc art. 8 ustawy o zakładowym funduszu świadczeń socjalnych. Po zmianie przepis ten ma zobowiązywać osoby uprawnione do korzystania z Funduszu do przekazywania swoich danych w formie oświadczenia.

Z projektu ustawy wprowadzającej RODO wynika, że pracodawca będzie mógł przetwarzać dane osób uprawnionych wyłącznie w celu i w zakresie niezbędnym do przyznania ulgowych usług i świadczeń oraz dopłat z Funduszu, a także do ustalenia ich wysokości. Projekt zobowiązuje go do przechowywania tych danych nie dłużej niż jest to niezbędne do realizacji tych celów oraz przez okres dochodzenia praw lub roszczeń, a także obliguje do uwzględnienia powyższych zasad w regulaminie Funduszu. Z racji bezpośredniego obowiązywania RODO, pracodawca powinien zmodyfikować postanowienia regulaminu, nie czekając na wejście w życie proponowanych rozwiązań krajowych, zwłaszcza, że ich treść jest skorelowana z RODO.

2) Czy drugi rodzic dziecka osoby uprawnionej do korzystania ze świadczeń Funduszu musi wyrazić zgodę na przetwarzanie danych tego dziecka?

NIE. Zgoda w tym przypadku nie jest wymagana. W razie korzystania ze świadczeń Funduszu nie chodzi bowiem o przetwarzanie danych dziecka w celach marketingowych, do tworzenia profilu osobowego lub użytkownika czy w celu kierowania usług bezpośrednio do niego, kiedy to działa szczególna ochrona danych dzie-

ka (motyw 38 preambuły RODO). Nie są to także usługi społeczeństwa informacyjnego, w stosunku do których wymagana jest zgoda rodzica lub opiekuna dziecka do 16. roku życia (art. 8 RODO). Tutaj podstawą działań pracodawcy są konkretne przepisy, wskazane w odpowiedzi na pytanie 1.

13. Ochrona danych w zakładzie pracy chronionej

Posiadamy status zakładu pracy chronionej. Zatrudniamy kilkadziesiąt pracowników, z których większość to niepełnosprawni. Czy po wejściu w życie RODO pracodawca musi prowadzić rejestr czynności przetwarzania danych osobowych oraz czy musi wyznaczyć inspektora ochrony danych?

Na podstawie art. 30 ust. 2 RODO pracodawcy są zobowiązani, jako administratorzy danych, do prowadzenia rejestru czynności przetwarzania. Obowiązek ten obejmuje podmioty zatrudniające co najmniej 250 osób. Podlegają mu też podmioty zatrudniające mniej osób, jeżeli przetwarzanie danych m.in.:

- nie ma charakteru sporadycznego,
- obejmuje tzw. dane wrażliwe (m.in. ujawniające pochodzenie rasowe lub etniczne, lub dotyczące zdrowia).

Zakład pracy chronionej, o którym mowa w pytaniu, musi więc prowadzić rejestr czynności przetwarzania danych, mimo że zatrudnia poniżej 250 osób. Przetwarza bowiem dane osobowe pracowników stale, a w przypadku tych z orzeczeniem o niepełnosprawności są to dodatkowo dane wrażliwe dotyczące zdrowia (art. 4 pkt 15 RODO).

Krąg podmiotów zobowiązanych do powołania inspektora

danych osobowych określa art. 37 ust. 1 w związku z motywem 97 preambuły RODO. Są to:

- organy lub podmioty publiczne (z wyjątkiem sądów w zakresie sprawowania wymiaru sprawiedliwości),
- podmioty, których główna działalność polega na przetwarzaniu danych, wymagających regularnego i systematycznego monitorowania osób na dużą skalę z uwagi na swój charakter, zakres lub cel,
- podmioty zajmujące się przede wszystkim przetwarzaniem na dużą skalę danych wrażliwych, w tym związanych ze stanem zdrowia.

W omawianej sytuacji zakład pracy chronionej raczej nie spełnia tych przesłanek. Nie ma więc obowiązku powoływania wspomnianego inspektora.

Podstawa prawna

Ustawa z dnia 26.06.1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917 ze zm.)