INFORLEX

poleca

e-book

ZMIANY DLA PRACODAWCÓW W USTAWIE O OCHRONIE DANYCH OSOBOWYCH OD 25 MAJA 2018 R.

stan prawny 21 czerwca 2018r.

Jadwiga Sztabińska

978-83-8137-356-2

30 LAT INFOR Zał. R. Pieńkowski w 1987 r.

Spis treści

Zmiany dla pracodawców w ustawie o ochronie danych osobowych od 25 maja 2018 r.

Zmiany dla pracodawców w ustawie o ochronie danych osobowych od 25 maja 2018 r.

Zobacz więcej www.inforakademia.pl

Od 25 maja 2018 r. obowiązuje nowa ustawa o ochronie danych osobowych. Wprowadziła ona zmiany do Kodeksu pracy regulujące zasady monitoringu pracowników, uzupełniła reguły wyznaczania inspektora ochrony danych oraz doprecyzowała tryb prowadzenia kontroli i nakładania kar za nieprzestrzeganie przepisów o ochronie danych osobowych.

Ustawa z 10 maja 2018 r. o ochronie danych osobowych (dalej ustawa o ochronie danych) jest rozwinięciem unijnego rozporządzenia 2016/679 (dalej RODO). Oznacza to, że pracodawcy muszą przestrzegać obu aktów prawnych, choć nie wszystkie regulacje mogą dotyczyć każdego z nich. Pracodawca może bowiem prowadzić monitoring pracowników, ale nie musi tego robić. Jeżeli go nie prowadzi, nie stosuje rozwiązań w tym zakresie i nie mają one dla niego żadnego znaczenia aż do czasu zmiany decyzji. Tak samo jest z inspektorem danych osobowych: albo pracodawca ma obowiązek powołania inspektora, albo nie – z tym że najpierw powinien sprawdzić, czy nie ma obowiązku jego powołania. Zupełnie inna sytuacja jest z kontrolą stosowania przepisów o ochronie danych osobowych i karami finansowymi za ich naruszenie. Tym przepisom podlega każdy pracodawca mający status administratora danych, którym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, ustalający samodzielnie lub wspólnie z innymi cele i sposoby przetwarzania danych osobowych. Podobnie jest w przypadku nowego organu nadzorczego w zakresie ochrony danych, tj. Urzędu Ochrony Danych Osobowych (UODO), który 25 maja 2018 r. zastąpił z mocy prawa Generalnego Inspektora Ochrony Danych Osobowych. UODO jest organem sprawującym nadzór nad przestrzeganiem przepisów o ochronie danych w przypadku wszystkich administratorów tych danych.

1. Nowe zasady dotyczące monitoringu pracowników

Do 25 maja 2018 r. monitoring w miejscu pracy nie był regulowany. Od tej daty pracodawcy, którzy monitorują teren zakładu pracy albo planują takie działanie, muszą postępować zgodnie z ogólnymi zasadami RODO oraz art. 22^2 i art. 22^3 Kodeksu pracy, które uregulowały prowadzenie monitoringu w zakładzie pracy.

Każda z form monitoringu może być wykorzystywana wyłącznie w ustawowo określonym celu oraz przy przestrzeganiu tajemnicy korespondencji, godności i innych dóbr osobistych pracowników – przedstawia to tabela na str. 39. W tym kontekście nadal pozostaje aktualna interpretacja Europejskiego Trybunału Praw Człowieka wyrażona w wyroku z 3 kwietnia 2007 r. w sprawie Copland przeciwko Wielkiej Brytanii (sygn. akt 62617/00). Trybunał uznał, że rozmowy telefoniczne z pracy, e-maile i użytkowanie Internetu podlegają pojęciom „życia prywatnego" i „tajemnicy korespondencji", w związku z czym ich kontrolowanie wymaga wyraźnej podstawy prawnej oraz poinformowania pracownika. Od 25 maja 2018 r. taką podstawą są art. 22^2–22^3 Kodeksu pracy. Regulują one zasady stosowania monitoringu wizyjnego pracowników i monitoringu poczty elektronicznej.

Cele monitoringu, zakazy i granice jego stosowania

Rodzaj monitoringu	Cele monitoringu	Zakaz stosowania	Granice stosowania
Rejestracja obrazu (tzw. monitoring wizyjny)	Monitoring wizyjny można wprowadzić jedynie, gdy jest to niezbędne do: – zapewnienia bezpieczeństwa pracowników, – ochrony mienia lub kontroli produkcji, – zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę	Monitoringu wizyjnego nie można stosować w: pomieszczeniach sanitarnych, szatniach, stołówkach oraz palarniach i pomieszczeniach udostępnianych zakładowej organizacji związkowej	Nagrywanie w pomieszczeniach objętych zakazem monitoringu jest dopuszczalne z powodu konieczności osiągnięcia podstawowych celów rejestracji obrazu – nie może jednak naruszać godności i innych dóbr osobistych pracownika oraz zasad wolności i niezależności związków zawodowych. Stąd powinny być wykorzystywane przynajmniej techniki uniemożliwiające rozpoznanie osób przebywających w tych pomieszczeniach
Kontrola służbowej poczty elektronicznej (monitoring poczty elektronicznej) **Sprawdzanie połączeń telefonicznych** **Nadzór aktywności internetowej**	Monitoring służbowej poczty elektronicznej oraz inne tego typu formy monitoringu mogą być stosowane, gdy jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy	Brak ustawowych wskazań	Obserwacja w tych trzech formach monitoringu nie może naruszać tajemnicy korespondencji i innych dóbr osobistych pracownika – pracodawcy nie wolno przeglądać prywatnych e-maili, słuchać rozmów o takim charakterze czy sprawdzać stron niemających związku z zadaniami służbowymi pracownika.

Monitoring pracowników wymaga nie tylko wdrożenia odpowiednich regulacji zakładowych, ale i ich spójności z zasadami określonymi w RODO (art. 5 w zw. z motywami 39–47, 58 i 60 preambuły RODO), tj.: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania danych, integralności i poufności oraz rozliczalności. Dodatkowo ustawa o ochronie danych osobowych nałożyła na pracodawców dodatkowe nakazy i obowiązki związane z wprowadzeniem i utrzymywaniem monitoringu.

1.1. Jak wdrożyć/zaktualizować monitoring

Nowe przepisy o monitoringu powodują konieczność przygotowania/zmiany zapisów odpowiednio w: układzie zbiorowym pracy (zakładowym lub ponadzakładowym), regulaminie pracy, a gdy pracodawca nie musi ich posiadać – w obwieszczeniu. W tych dokumentach

należy bowiem określić cel, zakres i sposób monitoringu (art. 22^2 § 6 Kodeksu pracy). Poniżej przedstawiamy procedurę wdrożenia (jeżeli pracodawca nie posiada przepisów o monitoringu, a chce monitorować pracowników) lub dostosowania przepisów wewnętrznych do regulacji dotyczących monitoringu pracowników.

Krok 1. Przygotowanie przepisów wewnątrzfirmowych

Treść obwieszczenia o monitoringu (wdrożeniu lub zmianie) pracodawca może ustalić samodzielnie, ponieważ w tym przypadku nie ma żadnych wymagań prawnych. Postanowienia układu zbiorowego pracy i regulaminu pracy muszą być natomiast uzgodnione z organizacjami związkowymi (art. 104^2 § 1 i art. 241^9 § 1 Kodeksu pracy). W odniesieniu do regulaminu pracy istnieje jednak opcja autonomicznej decyzji pracodawcy. Wystąpi, gdy w ustawowym, 30-dniowym lub wyznaczonym wspólnie z organizacjami związkowymi terminie nie uda się osiągnąć porozumienia albo w firmie nie ma związku zawodowego. Taki wariant nie istnieje przy układzie zbiorowym – brak ustalenia regulacji ze związkami powoduje, że nie dochodzi do ich wprowadzenia/aktualizacji.

UWAGA!

Pracodawca powinien poinformować pracowników o wprowadzeniu monitoringu na co najmniej 2 tygodnie przed jego uruchomieniem.

Krok 2. Poinformowanie pracowników

Bez względu na rodzaj stosowanych przepisów wewnątrzfirmowych pracodawca ma obowiązek poinformować pracowników o wprowadzeniu monitoringu na co najmniej 2 tygodnie przed jego uruchomieniem (art. 22^2 § 7 Kodeksu pracy). Mimo że nowe rozwiązania kodeksowe nie nakazują zawiadamiania pracowników o zmianie regulacji dotyczących zasad monitorowania, należy przyjąć, że pracodawca jest do tego zobligowany na podstawie art. 104^3 § 1 i art. 241^{12} § 1 Kodeksu pracy. Regulacje te pomijają obwieszczenie, ale tu obowiązek informacyjny ma swoje podstawy w art. 13, art. 5 ust. 1 lit. a oraz motywie 39 preambuły RODO, choć nie jest wskazany termin jego wykonania.

Poinformowanie pracowników powinno nastąpić w sposób przyjęty u danego pracodawcy, np. poprzez powieszenie informacji na tablicy ogłoszeń, jej przesłanie do służbowych skrzynek e-mailowych pracowników (jeśli wszyscy je posiadają) czy udostępnienie w intranecie. Informacja ma być napisana jasnym i prostym językiem, dzięki czemu jej treść będzie przejrzysta, zwięzła i zrozumiała (art. 12 ust. 1 RODO).

Krok 3. Termin obowiązywania regulacji o monitoringu

Nie ma jednego terminu, w którym zmienione/nowe przepisy wewnątrzfirmowe dotyczące monitoringu wejdą w życie. W przypadku regulaminu pracy nastąpi to po upływie 2 tygodni od ich podania do wiadomości pracowników. Natomiast protokół dodatkowy do układu zbiorowego wejdzie w życie w terminie w nim ustalonym, ale nie wcześniej niż z dniem zarejestrowania protokołu. Co do obwieszczenia nie ma żadnych prawnych wytycznych, a zatem pracodawca samodzielnie o tym decyduje. Obwieszczenie takie nie jest bowiem traktowane jak obwieszczenie o systemach i rozkładach czasu pracy.

Przykład obwieszczenia o wprowadzeniu monitoringu

Obwieszczenie dotyczące monitoringu

1. Na podstawie art. 22^2 i art. 22^3 Kodeksu pracy w związku z art. 5 i art. 6 ust. 1 lit. c i lit. f 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 (Dz.Urz.UE.L.2016.119.1) wprowadza się monitoring:
   a) rejestracji obrazu (tzw. monitoring wizyjny) w pomieszczeniach serwisowych i magazynowych w celu kontroli procesu realizacji usług, przestrzegania przepisów bezpieczeństwa i higieny pracy oraz ochrony mienia przed kradzieżą,
   b) służbowej poczty elektronicznej u wszystkich pracowników w celu kontroli czasu pracy oraz wykorzystywania tej poczty do realizacji zadań służbowych,
   c) połączeń telefonicznych z urządzeń stacjonarnych i komórkowych wszystkich pracowników w celu kontroli czasu pracy oraz wykorzystywania aparatów telefonicznych do potrzeb służbowych,
   d) służbowej aktywności internetowej pracowników mających dostęp do Internetu w celu kontroli czasu pracy oraz wykorzystywania połączeń on-line na potrzeby służbowe.
2. Wszystkie pomieszczenia objęte monitoringiem wizyjnym są oznakowane w postaci tabliczek z informacją o rejestracji obrazu, umieszczonych przed wejściem do pomieszczenia oraz wyjściem z niego. Informacja o monitoringu wizyjnym jest też umieszczona w pomieszczeniach obsługi klientów.
3. Monitoring będzie prowadzony z zachowaniem tajemnicy korespondencji, poszanowaniem godności i innych dóbr osobistych pracowników.
4. Materiały z monitoringu będą wykorzystywane wyłącznie w celach określonych w pkt 1.
5. Dostęp do materiałów z monitoringu będą miały wyłącznie osoby upoważnione do przetwarzania zawartych w nich danych. Na osobach upoważnionych spoczywa obowiązek zachowania w tajemnicy tych danych przez czas nieokreślony.
6. Nagrania z monitoringu wizyjnego będą przechowywane przez okres nieprzekraczający 3 miesięcy, licząc od dnia ich powstania, a materiały z pozostałych form monitoringu – 20 dni od otrzymania (billingi telefoniczne) lub wytworzenia (raport aktywności). Po upływie tych okresów materiały będą niszczone w sposób uniemożliwiający ich odtworzenie, pod warunkiem że nie powstanie potrzeba ich zatrzymania do czasu zakończenia określonego postępowania, w którym będą stanowić dowód.
7. Pracownikowi, którego dane znajdują się w materiałach z monitoringu, przysługuje prawo: dostępu do danych, ich prostowania i usuwania, ograniczenia przetwarzania i przenoszenia, a także wniesienia sprzeciwu do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.
8. Obwieszczenie obowiązuje od 1 września 2018 r.

1.2. Nowe obowiązki pracodawców w zakresie monitoringu

Pierwszym nowym obowiązkiem pracodawcy jest wykorzystywanie nagrań z monitoringu wizyjnego wyłącznie do celów, dla których został wprowadzony. Tylko ta forma nadzoru została zapisana wprost w nowych przepisach kodeksowych, ale ograniczenie celu odnosi się także do pozostałych rodzajów monitorowania, tyle że na podstawie RODO (art. 5 ust. 1 lit. b RODO).

Drugi nowy obowiązek to ograniczanie okresu przechowywania danych pozyskanych z monitoringu do minimum adekwatnego do celu przetwarzania. Jedynie w stosunku do nagrań okres ten został wyraźnie wskazany jako nieprzekraczający 3 miesięcy od dnia nagrania, a gdy jest ono dowodem w postępowaniu (np. sądowym albo administracyjnym) – okres przechowywania nagrania może zostać przedłużony do prawomocnego zakończenia postępowania (art. 22^2 § 3 Kodeksu pracy). Po upływie tego czasu pracodawca musi je zniszczyć, jeśli odrębne przepisy nie stanowią inaczej.

Trzeci nowy obowiązek to oznaczenie monitorowanych pomieszczeń i terenu w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem. Należy uznać, że dotyczy to także pracodawców korzystających z monitoringu przed 25 maja 2018 r., mimo że przepisy tego wprost nie określają.

Czwartym nowym obowiązkiem jest poinformowanie pracowników na piśmie przed dopuszczeniem do pracy o celach, zakresie i sposobie monitoringu (art. 22^2 § 8 Kodeksu pracy).

Przykład informacji o wprowadzeniu monitoringu

Warszawa, 1 sierpnia 2018 r.

Sprawne auto Sp. z o.o.

W miejscu

INFORMACJA O WPROWADZENIU MONITORINGU

Informuję, że z dniem 1 września 2018 r. zostanie wprowadzony monitoring polegający na:

– rejestracji obrazu w pomieszczeniach serwisowych i magazynowych,

– kontroli służbowej poczty elektronicznej wszystkich pracowników,

– kontroli połączeń telefonicznych z aparatów stacjonarnych i komórkowych wszystkich pracowników,

– kontroli aktywności internetowej pracowników mających dostęp do Internetu.

Treść obwieszczenia o wprowadzeniu monitoringu jest dostępna w intranecie w zakładce „Regulacje wewnętrzne".

Pytania w tej sprawie można kierować do zarządu w każdym trybie: telefonicznym, e-mailowym lub osobistym.

Jan Kowalski

Prezes zarządu

Marian Nowicki

Wiceprezes zarządu

PRZYKŁAD
Pracodawca działający w obszarze usług (serwis aut) zamierza wprowadzić od 1 września 2018 r. cztery formy monitoringu: wizyjny, poczty elektronicznej, służbowych telefonów stacjonarnych i komórkowych oraz korzystania z Internetu. Z uwagi na brak związków zawodowych, układu zbiorowego pracy i obowiązku posiadania regulaminu pracy obwieszczenie przygotowuje samodzielnie. Musi pamiętać, aby poinformować pracowników o swoich planach monitorowania nie później niż do 18 sierpnia 2018 r. (2 tygodnie przed uruchomieniem) i oznakować monitorowane pomieszczenia najpóźniej 31 sierpnia 2018 r.

2. Inspektor ochrony danych

Wyznaczenia inspektora danych osobowych (IOD) w miejsce dotychczasowych administratorów bezpieczeństwa informacji (ABI) mają dokonać:

- organy lub podmioty publiczne, tj. jednostki sektora finansów publicznych, instytuty badawcze i Narodowy Bank Polski, 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, tj. pracodawcy, których zasadniczym (nie pobocznym) zadaniem jest przetwarzanie danych,
- podmioty zajmujące się przede wszystkim przetwarzaniem na dużą skalę danych wrażliwych (ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności czy orientacji seksualnej tej osoby) oraz danych dotyczących wyroków skazujących i naruszeń prawa. Według Grupy Roboczej Art. 29 (jest to unijny niezależny organ doradczy) duża skala odnosi się m.in. do szpitali, transportu publicznego, fast foodów, banków, ubezpieczycieli, firm zajmujących się reklamą behawioralną przez wyszukiwarki internetowe, dostawców usług internetowych i telefonicznych

(art. 37 ust. 1 w zw. z art. 9 ust. 1 i motyw 97 preambuły RODO oraz art. 8–9 ustawy o ochronie danych).

Dla wykonania tego obowiązku nie ma znaczenia liczba osób zatrudnionych przez pracodawcę. Bez wpływu pozostaje ona także na decyzję pracodawców ze sfery pozabudżetowej, którzy nie mieszczą się na powyższej liście, a u których powołanie IOD jest dobrowolne.

Ustanowienie IOD jest jednak warte rozważenia ze względu na wiedzę o ochronie danych osobowych, którą inspektor może służyć, i zadania, które wykonuje. Można też zdecydować się na wyznaczenie IOD przez grupę przedsiębiorstw, co jest w pełni dopuszczalne. Mogą to zrobić również pracodawcy ze sfery publicznej.

Kwalifikacje, zadania i status inspektora danych osobowych

Kwalifikacje i umiejętności	Zadania i obowiązki	Status prawny
Znajomość krajowych, unijnych i europejskich przepisów oraz praktyk w zakresie ochrony danych	Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych europejskich (w tym krajowych) przepisów o ochronie danych, a także doradzanie im w tej sprawie	Niezależność przy wykonywaniu zadań i obowiązków – administrator danych (pracodawca) i podmiot przetwarzający dane nie wskazują sposobu wykonywania zadań przez IOD
Znajomość prowadzonych operacji przetwarzania danych, stosowanych technologii informatycznych i bezpieczeństwa danych	Monitorowanie przestrzegania RODO i innych europejskich (w tym krajowych) przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych	Brak możliwości odwołania przez administratora (pracodawcę) i podmiot przetwarzający lub otrzymania od nich kary z tytułu wykonywania zadań IOD
Umiejętności promowania kultury ochrony danych wewnątrz organizacji	Podejmowanie działań zwiększających świadomość, organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania oraz prowadzenie powiązanych z tym audytów	Bezpośrednie podleganie najwyższemu kierownictwu administratora (pracodawcy) lub podmiotowi przetwarzającemu
Umiejętność współpracy	Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania	Zapewnione wsparcie w postaci zasobów niezbędnych do wykonania zadań i utrzymania wiedzy oraz dostęp do danych osobowych i operacji przetwarzania
	Pełnienie funkcji punktu kontaktowego dla UODO w kwestiach związanych z przetwarzaniem danych, w tym z uprzednimi konsultacjami przed podjęciem przetwarzania danych o wysokim ryzyku, a także prowadzenie konsultacji we wszelkich innych sprawach	Zagwarantowanie ze strony administratora (pracodawcy) oraz podmiotu przetwarzającego właściwego i niezwłocznego włączania IOD we wszystkie sprawy dotyczące ochrony danych osobowych
	Utrzymywanie pozycji kontaktowej we wszystkich sprawach związanych z przetwarzaniem danych osób, których dane osobowe dotyczą, oraz z wykonywaniem przysługujących praw	
	Zachowanie tajemnicy lub poufności co do wykonywania swoich zadań	
	Wykonywanie innych zadań i obowiązków, pod warunkiem że nie powodują konfliktu interesów	
	Współpraca z UODO	

Z wyznaczeniem IOD wiążą się określone obowiązki pracodawcy. Poniżej przedstawiamy, jak powinien on postępować w tej sprawie, bez względu na to, czy powołanie IOD następuje obowiązkowo czy dobrowolnie.

2.1. Procedura związana z wyznaczeniem IOD

Krok 1. Wybór odpowiedniego kandydata

Pracodawca może powierzyć zadania IOD osobie:

- ze swojego personelu (nie powinna ona jednocześnie zajmować się systemami informatycznymi albo przetwarzaniem danych w danym obszarze, np. kadrowym, aby nie powstał konflikt interesów),
- zatrudnionej w podmiocie przetwarzającym dane pracowników, jeśli pracodawca powierzył mu przetwarzanie danych,
- spoza struktur własnych i podmiotu przetwarzającego – na umowę o świadczenie usług.

UWAGA!

Pracodawca musi wyznaczyć inspektora ochrony danych do 31 lipca 2018 r., jeżeli ma taki obowiązek.

Jeśli pracodawca ma w swojej strukturze ABI, to osoba pełniąca tę funkcję 24 maja 2018 r. stała się z dniem następnym IOD (art. 158 ust. 1 ustawy o ochronie danych). Może zajmować to stanowisko do 1 września 2018 r., chyba że przed tym dniem pracodawca zawiadomi UODO o wyznaczeniu innej osoby. Niewykluczone jest też, że po tej dacie nadal będzie wykonywać zadania IOD, jeśli pracodawca właśnie ją wskaże w zawiadomieniu składanym do UODO do 1 września 2018 r. Możliwa jest też inna sytuacja, tj. utrata stanowiska po 24 maja 2018 r. bez informowania o tym UODO. Stanie się tak, jeśli pracodawca nie jest zobligowany do powołania IOD i nie zamierza tego uczynić dobrowolnie.

Pracodawca musi wyznaczyć IOD do 31 lipca 2018 r., jeśli ma taki obowiązek, a dotychczas nie było u niego ABI. Do tego dnia musi też zawiadomić o wyborze UODO. Te same nakazy dotyczą podmiotu przetwarzającego dane pracowników.

PRZYKŁAD

U pracodawcy działającego w sferze ubezpieczeń funkcję administratora bezpieczeństwa informacji pełniła osoba z zewnątrz. Stała się z dniem 25 maja 2018 r. inspektorem ochrony danych osobowych i utrzyma tę pozycję przez czas nieokreślony. Pracodawca jest bowiem zadowolony ze współpracy z nią, w związku z czym zawiadomił w czerwcu 2018 r. Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu tej osoby na stanowisko IOD.

Krok 2. Zawiadomienie UODO

Pracodawca ma 14 dni od dnia wyznaczenia (zmiany) IOD na poinformowanie o tym fakcie UODO, również wtedy, gdy do powołania jednego IOD doszło w grupie przedsiębiorstw/podmiotów publicznych. Zawiadomienie powinno zawierać: imię i nazwisko tej osoby, adres poczty elektronicznej i numer telefonu, a także własne dane pracodawcy: nazwę, adres siedziby i REGON (jeśli go posiada), a gdy jest osobą fizyczną, podaje: imię i nazwisko, adres zamieszkania; w przypadku osoby fizycznej prowadzącej działalność gospodarczą – firmę (nazwę) przedsiębiorstwa i adres prowadzenia działalności gospodarczej.

Zawiadomienie ma być sporządzone w postaci elektronicznej i zaopatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Gdy pracodawca składa je przez pełnomocnika, dołącza pełnomocnictwo w formie elektronicznej. Formularze zawiadomień są dostępne na uodo.gov.pl.

PRZYKŁAD
Grupa pracodawców prowadzących fast foody zdecydowała o powołaniu jednego IOD. Wcześniej żaden z nich nie miał w zakładzie ABI. Każdy z pracodawców osobno ma czas na zgłoszenie do UODO wyznaczonego IOD do 31 lipca 2018 r.

Krok 3. Udostępnienie danych IOD

Niezwłocznie po wyznaczeniu IOD pracodawca udostępnia jego dane na swojej stronie internetowej, a gdy jej nie prowadzi – w sposób ogólnie dostępny w miejscu prowadzenia działalności (art. 11 ustawy o ochronie danych). Jego dane kontaktowe umieszcza także w klauzulach informacyjnych dla pracowników i kandydatów do pracy oraz w rejestrze czynności przetwarzania i zgłoszeniu naruszenia ochrony danych.

3. Kontrola przestrzegania przepisów o ochronie danych

UODO będzie prowadził kontrole przestrzegania przepisów o ochronie danych osobowych według zatwierdzonego planu lub na podstawie uzyskanych informacji albo w ramach monitorowania stosowania RODO. Pracodawca może spodziewać się pracownika polskiego urzędu lub organu nadzorczego innego państwa UE, posiadającego imienne upoważnienie, w którym mają być zawarte:

- imię i nazwisko, stanowisko służbowe kontrolującego oraz numer legitymacji służbowej, a w przypadku kontrolującego obcokrajowca – imię i nazwisko oraz numer dokumentu potwierdzającego tożsamość,
- podstawa prawna kontroli i jej zakres,
- organ kontrolujący i podmiot kontrolowany,
- data rozpoczęcia i przewidywany termin zakończenia czynności kontrolnych (dzień podpisania protokołu kontroli przez kontrolowanego lub sporządzenia wzmianki w protokole przez kontrolującego o odmowie jego podpisania), co ma trwać nie dłużej niż 30 dni od dnia okazania kontrolowanemu imiennego upoważnienia oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość,
- pouczenie o prawach kontrolowanego,
- data i miejsce jego wystawienia,
- podpis Prezesa UODO.

Kontrola rozpoczyna się po okazaniu tego dokumentu (upoważnienia) oraz legitymacji służbowej lub dokumentu potwierdzającego tożsamość. Ma być wykonywana w obecności kontrolowanego lub osoby przez niego upoważnionej (art. 83 ustawy o ochronie danych). W jej trakcie kontrolujący może wykonywać przysługujące mu ustawowo prawa, a kontrolowany pracodawca musi realizować nałożone na niego przepisami obowiązki – zob. tabela na str. 47. Po zakończeniu kontroli zostanie sporządzony protokół kontroli, w dwóch egzemplarzach, w postaci elektronicznej lub papierowej, zawierający m.in. opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Protokół powinien być podpisany przez kontrolującego i kontrolowanego, a jeśli ten ostat-

ni odmówi (tak też będzie traktowane nieprzekazanie podpisanego dokumentu w terminie 7 dni od jego otrzymania) – zostanie poczyniona wzmianka na ten temat. Ewentualne zastrzeżenia pracodawcy mogą spowodować dodatkowe czynności kontrolne i zmianę/pozostawienie bez zmian treści dokumentu. Mogą też zostać nieuwzględnione, a wtedy pracodawca otrzymuje uzasadnienie tej decyzji.

Kontrole wszczęte i niezakończone do 25 maja 2018 r. są prowadzone na podstawie poprzednich przepisów. Upoważnienia i legitymacje służbowe wydane przed tą datą zachowują swoją ważność do czasu zakończenia takich kontroli.

Prawa kontrolującego i obowiązki kontrolowanego pracodawcy

Prawa kontrolującego	Obowiązki kontrolowanego pracodawcy
Wstęp w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń kontrolowanego pracodawcy	Wskazanie na piśmie osoby upoważnionej do reprezentowania pracodawcy w trakcie kontroli
Wgląd do dokumentów i informacji mających bezpośredni związek z zakresem kontroli (w tym objętych tajemnicą prawnie chronioną, jeśli przepisy szczególne nie stanowią inaczej) oraz żądanie tłumaczenia na język polski dokumentów sporządzonych w obcym języku	Zapewnienie kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunków i środków niezbędnych do sprawnego przeprowadzenia kontroli, a w szczególności sporządzanie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach
Przeprowadzanie oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych	Dokonywanie potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków
Żądanie złożenia pisemnych lub ustnych wyjaśnień oraz prawo przesłuchiwania w charakterze świadka zatrudnionych u kontrolowanego w zakresie niezbędnym do ustalenia stanu faktycznego	
Zlecanie ekspertyz i opinii	
W uzasadnionych przypadkach utrwalanie przebiegu kontroli lub jej poszczególnych czynności za pomocą urządzeń rejestrujących obraz lub dźwięk, po uprzednim poinformowaniu kontrolowanego	
Korzystanie z pomocy Policji w uzasadnionych przypadkach, np. gdy pracodawca uniemożliwia kontrolę	

4. Kary za naruszenie przepisów o ochronie danych

Informacje zgromadzone podczas kontroli mogą stanowić podstawę do wszczęcia postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. Takie postępowania prowadzi Prezes UODO w każdym przypadku podejrzenia działania wbrew prawu (art. 60–74 ustawy o ochronie danych). Kończy je wydaniem decyzji. W jej uzasadnieniu wskazuje przesłanki z art. 83 ust. 2 RODO, które stały się podstawą do nałożenia administracyjnej kary pieniężnej oraz ustalenia jej wysokości, m.in. charakter, wagę i czas trwania naruszenia z uwzględnieniem charakteru, zakres lub cel danego przetwarzania, liczbę

poszkodowanych osób, których dane dotyczą, oraz rozmiar poniesionej przez nie szkody, a także umyślność/nieumyślność działania pracodawcy. Pracodawca może odwołać się od decyzji do sądu administracyjnego, co wstrzyma jej wykonanie.

Jeśli przemawia za tym interes publiczny, Prezes UODO opublikuje decyzję na swojej stronie internetowej w Biuletynie Informacji Publicznej.

Ukarany pracodawca musi uiścić karę w ciągu 14 dni od dnia upływu terminu na wniesienie skargi albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego (art. 105 ust. 1 ustawy o ochronie danych). Wolno mu jednak wnioskować o odroczenie terminu jej uregulowania albo rozłożenie na raty, jeśli ma ważny interes przemawiający za taką prośbą, który musi wskazać w uzasadnieniu. Przy pozytywnej decyzji Prezesa UODO (formalnie: postanowienie) pracodawca będzie musiał zapłacić odsetki (z zastosowaniem odsetek za zaległości podatkowe) od niewpłaconej kwoty:

- od dnia następującego po dniu złożenia wniosku; w przypadku rozłożenia na raty odsetki będą naliczane odrębnie dla każdej raty,
- od dnia upływu odroczonego terminu uiszczenia kary albo terminu uiszczenia poszczególnych rat – w razie niedotrzymania tych terminów.

Taka decyzja może być uchylona, jeśli ujawnią się nowe albo uprzednio nieznane okoliczności istotne dla rozstrzygnięcia lub jeżeli pracodawca nie zapłaci terminowo raty.

Maksymalna wysokość administracyjnych kar finansowych za naruszenie przepisów o ochronie danych osobowych

Karany podmiot	Maksymalny poziom kary	Rodzaj naruszenia
1	2	3
Jednostki sektora finansów publicznych, instytuty badawcze i NBP	100 tys. zł	Brak rozróżnienia
Państwowe i samorządowe jednostki kultury	10 tys. zł	Brak rozróżnienia
Inne podmioty niż wymienione powyżej, z wyjątkiem przedsiębiorców	10 mln euro*	Obowiązki administratora danych dotyczących uzyskiwania zgód, przetwarzania danych niewymagających identyfikacji, obowiązków ogólnych i związanych z bezpieczeństwem danych oraz oceną skutków i IOD (art. 25–39 RODO), a także obejmujących certyfikację i monitorowanie przestrzegania RODO
	20 mln euro*	■ Podstawowe zasady przetwarzania danych (w tym danych wrażliwych) i warunki zgód ■ Prawa osób, których dane są przetwarzane, określone w art. 12–22 RODO ■ Przekazywanie danych do państw trzecich lub organizacji międzynarodowych ■ Obowiązki wynikające z przetwarzania danych w szczególnych sytuacjach, zgodnie z rozdziałem IX RODO

1	2	3
		■ Nieprzestrzeganie nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania, lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy, lub niezapewnienia dostępu do danych
Przedsiębiorcy	2% całkowitego rocznego światowego obrotu za poprzedni rok obrotowy	Obowiązki administratora danych dotyczących uzyskiwania zgód, przetwarzania danych niewymagających identyfikacji, obowiązków ogólnych i związanych z bezpieczeństwem danych oraz oceną skutków i IOD (art. 25–39 RODO), a także obejmujących certyfikację i monitorowanie przestrzegania RODO
	4% całkowitego rocznego światowego obrotu za poprzedni rok obrotowy	■ Podstawowe zasady przetwarzania danych (w tym danych wrażliwych) i warunki zgód ■ Prawa osób, których dane są przetwarzane, określone w art. 12–22 RODO ■ Przekazywanie danych do państw trzecich lub organizacji międzynarodowych ■ Obowiązki wynikające z przetwarzania danych w szczególnych sytuacjach, zgodnie z rozdziałem IX RODO ■ Nieprzestrzeganie nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania, lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy, lub niezapewnienia dostępu do danych

** Karę oblicza się w złotych według średniego kursu euro NBP z tabeli kursów na 28 stycznia każdego roku, a gdy w danym roku NBP nie ogłasza średniego kursu euro 28 stycznia – według średniego kursu euro ogłoszonego w najbliższej po tej dacie tabeli kursów.*

Administracyjne kary pieniężne nie są jedynymi sankcjami za działania wbrew regulacjom o ochronie danych osobowych. Temu, kto takie dane przetwarza mimo niedopuszczalności lub bez uprawnienia, grozi grzywna, ograniczenie wolności albo pozbawienie wolności do 2 lat, a do 3 lat – gdy są to dane wrażliwe. Takie same kary (z wyjątkiem pozbawienia wolności do lat 3) dotyczą pracodawcy, który utrudnia kontrolującemu prowadzenie kontroli (art. 108 ustawy o ochronie danych). Oprócz tego pracodawcom grożą roszczenia cywilne od pracowników, kandydatów do pracy i innych osób, które będą uważały, że doszło do naruszenia ochrony ich danych osobowych lub że poniosły szkodę z tego powodu (art. 92 ustawy o ochronie danych w zw. z art. 79 i art. 82 RODO).

Podstawa prawna:

- motyw 39–47, motyw 58, motyw 60, motyw 97 preambuły oraz art. 4 pkt 7, art. 5, art. 6 ust. 1, art. 7, art. 8, art. 9 ust. 1, art. 10–22, art. 25–39, art. 41–43, art. 79, art. 82, art. 83 ust. 2, 4 i 5 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 – Dz.Urz. UE. L. z 2016 r. nr 119, str. 1
- art. 8–11, art. 60–74, art. 78–92, art. 101–108, art. 111, art. 158, art. 159, art. 166 ustawy z 10 maja 2018 r. o ochronie danych osobowych – Dz.U. z 2018 r. poz. 1000
- art. 22^2, art. 22^3, art. 104^2 § 1, art. 104^3 § 1, art. 150, art. 241^9 § 1, art. 241^{12} § 1 ustawy z 26 czerwca 1974 r. – Kodeks pracy – j.t. Dz.U. z 2018 r. poz. 917; ost.zm. Dz.U. z 2018 r. poz. 1076

©℗
Jadwiga Sztabińska
prawnik specjalizujący się w prawie pracy, w tym z zakresu sfery budżetowej