

29

Obowiązki pracodawcy i pracownika w zakresie ochrony danych osobowych

POZNASZ

- podstawy prawne regulujące ochronę danych osobowych;
- pojęcia związane z ochroną danych osobowych;
- zasady postępowania w obiegu informacji zawierających dane osobowe.

Ochrona danych osobowych jest tematem, w obszarze którego w ostatnim czasie wiele się zmieniło. Od 25 maja 2018 r. przestała obowiązywać dotychczasowa *Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych*, a jej miejsce zastąpiła *Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych* (DzU z 2018 r. poz. 1000), która wprowadza wiele zmian i gwarantuje większą kontrolę nad naszymi danymi osobowymi w sieci. Ustawa dotycząca RODO jest wynikiem wydane-go przez Parlament Europejski i Radę Unii Europejskiej rozporządzenia w sprawie ochrony danych osobowych. „RODO”, inna nazwa „GDPR” lub „Ogólne Rozporządzenie o Ochronie Danych” to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Rozporządzenie dotyczy wszystkich przetwarzających dane osobowe w związku z prowadzoną działalnością gospodarczą.

Nowością wprowadzoną przez RODO są **kodeksy postępowania** (tzw. kodeksy dobrych praktyk), które mają pomóc we właściwym jego stosowaniu. Rozporządzenie zachęca zrzeczenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające do tworzenia kodeksów postępowania, przy uwzględnieniu specyfiki różnych sektorów przetwarzających dane oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Nowa ustawa nakłada wymóg uprzednich konsultacji kodeksu przed przekazaniem go do zatwierdzenia przez Prezesa UODO (Urzędu Ochrony Danych Osobowych). Informację o przeprowadzonych konsultacjach i ich wyniku oraz przygotowany kodeks postępowania przekazuje się organowi nadzorcemu do zatwierdzenia.

Kolejną zmianą w dotychczas obowiązującym stanie prawnym jest **certyfikacja**. Zgodnie z ustawą, podmiotom ubiegającym się o uprawnienia do nadawania certyfikacji, czyli pewnych korzyści a zarazem obowiązków dla administratora danych, akredytacji udziela Polskie Centrum Akredytacji. Akredytacji można udzielić maksymalnie na okres 5 lat. Natomiast certyfikacji na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek dokonuje Prezes UODO bądź podmiot certyfikujący (który uprzednio uzyskał akredytację Polskiego Centrum Akredytacji). Wniosek o certyfikację powinien być rozpatrzony w czasie nie dłuższym niż trzy miesiące od jego złożenia. Na stronie BIP Urzędu Ochrony Danych Osobowych (UODO) opublikowane są kryteria certyfikacji oraz wysokość opłaty związanych z jej udzieleniem. Jednocześnie Prezes UODO prowadzić będzie publiczny wykaz podmiotów, które uzyskały certyfikację oraz podmiotów, którym certyfikację cofnięto. Ponadto, ustawodawca przyznał organowi nadzorcemu możliwość przeprowadzania czynności sprawdzających skierowanych zarówno wobec podmiotu starającego się o przyznanie certyfikacji, jak i podmiotu, który już taką certyfikację uzyskał w celu oceny spełniania przez ten podmiot kryteriów certyfikacji. Administratorzy i podmioty przetwarzające dane są zobowiązane do powołania Inspektora Ochrony Danych. Nowa ustawa doprecyzowuje, że do organów i podmiotów publicznych obowiązanych do wyznaczenia IOD należy zaliczyć jednostki sektora finansów publicznych, instytuty badawcze oraz Narodowy Bank Polski. Podmiot, który wyznaczył Inspektora Ochrony Danych ma obowiązek udostępnienia imienia, nazwiska, adresu e-mail bądź numeru telefonu IOD na swojej stronie internetowej lub (w przypadkach, gdy podmiot nie ma własnej strony internetowej) w sposób ogólnie dostępny w miejscu prowadzenia działalności. Ustawa doprecyzowuje ponadto, że do roszczeń z tytułu naruszenia przepisów RODO należy stosować przepisy Kodeksu cywilnego, a właściwym organem do rozpatrywania roszczeń z tego tytułu jest sąd okręgowy. Odpowiednio do postępowań w tym zakresie stosuje się Kodeks postępowania cywilnego.

Nową ustawą o ochronie danych osobowych wprowadzono także zmiany w innych przepisach. Na szczególną uwagę zasługują zmiany w zakresie legalności **monitoringu**. Zmiany w powyższym zakresie dotyczą głównie **Kodeksu pracy**. Do tego aktu wprowadzono regulację, zgodnie z którą pracodawca może wprowadzić szczególnie nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring), jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników, ochrony mienia lub kontroli produkcji, jak również zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę (patrz art. 222 §1 Kp). Monitoringiem nie można objąć pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób (art. 222 §2 Kp). Pracodawca może przetwarzać nagrania obrazu wyłącznie w celach, dla których zostały zebrane i przechowywać nagrania maksymalnie przez 3 miesiące. Jest on zobowiązany także do poinformowania swoich pracowników o monitoringu nie później niż 2 tygodnie przed jego uruchomieniem oraz do oznaczenia pomieszczeń i terenów monitorowanych najpóźniej dzień przed jego uruchomieniem. Ponadto krajowy ustawodawca wprowadził analo-

giczne zasady wprowadzania monitoringu służbowej poczty elektronicznej pracownika, w sytuacjach gdy jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Przy tym monitoring nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Podobne zasady dotyczą także innych form monitoringu (m.in. gps). W pewnym uogólnieniu można stwierdzić, że w tym wypadku istotny jest cel, jakiemu służy monitoring. W pierwszym przypadku (obraz) chodzi o bezpieczeństwo szeroko rozumiane, w drugim o nadzór nad narzędziami, jakich używa pracownik celem weryfikacji efektywności ich użycia.

Jednocześnie ustawodawca uregulował także kwestię monitoringu stosowanego przez gminy i powiaty. Celem zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej mogą one stosować środki techniczne umożliwiające rejestrację obrazu (monitoring) w obszarze przestrzeni publicznej. Odbywać to się może za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy lub jednostek organizacyjnych gminy/powiatu, a także na terenie wokół takich nieruchomości i obiektów budowlanych. Warunkiem niezbędnym jest konieczność zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej. Monitoringu nie można uruchamiać w pomieszczeniach sanitarnych, szatniach, stołówkach, palarniach i obiektach socjalnych. Nagrania należy usunąć maksymalnie po trzech miesiącach od nagrania. Należy także zamieścić na nieruchomościach monitorowanych informację o nim.

Podobne wymogi wprowadzono także w ustawie o zasadach zarządzania mieniem państwowym oraz ustawie o samorządzie wojewódzkim. Jako warunek legalizujący stosowanie monitoringu, krajowy ustawodawca wskazał konieczność zapewnienia bezpieczeństwa zarządzanym mieniem państwowym, a w przypadku województwa także dodatkowo obowiązek zachowania szczególnej staranności przy wykonywaniu zarządu zgodnie z przeznaczeniem tego mienia i jego ochrona.

Omawianą ustawą wprowadzono również nowe przepisy w Prawie oświatowym, zgodnie z którymi dyrektor szkoły lub placówki w uzgodnieniu z organem prowadzącym szkołę lub placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić monitoring nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki, o ile wykaże, że jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia.

Ważne przy tym jest to, że – jak wskazał krajowy ustawodawca – monitoring nie powinien stanowić środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły lub placówki. Ponadto, co do zasady monitoring nie może obejmować pomieszczeń, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, pomieszczeń, w których uczniom jest udzielana pomoc psychologiczno-pedagogiczna oraz tych przeznaczonych do odpoczynku i rekreacji pracowników, sanitarno-higienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni. Wyjątkowo można monitorować ww. pomieszczenia, gdy jest to niezbędne ze względu na istniejące zagrożenie dla realizacji celu zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia i nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób. Jako przykład ustawodawca wskazuje zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Nagrania zawierające dane osobowe uczniów, pracowników i innych osób, których tożsamość można zidentyfikować, przetwarzane będą wyłącznie do celów, dla których zostały zebrane i usunąć najpóźniej trzy miesiące od dnia nagrania. Dyrektor szkoły lub placówki jest zobowiązany poinformować uczniów i pracowników o wprowadzeniu monitoringu najpóźniej 14 dni przed jego uruchomieniem. Pomieszczenia i teren monitorowany muszą być oznaczone w sposób czytelny i widoczny najpóźniej dzień przed uruchomieniem. Odnosnie nowo zatrudnionych ustawodawca wprowadził wymóg poinformowania ich na piśmie o monitoringu przed rozpoczęciem wykonywania obowiązków.

Podsumowując, należy wskazać na podstawowy cel RODO, czyli ochronę wszelkich danych osobowych rozumianą jako ochronę informacji dotyczących osób fizycznych przez podmioty, które nimi dysponują. Chodzi tutaj zarówno o pojedyncze informacje stanowiące dane osobowe, jak również o całe zbiory danych. Obowiązek ten wynika z zapisu wyżej przedstawionych przepisów, gdyż każda osoba ma prawo do ochrony swoich danych osobowych. Ochrona danych osobowych, to zabezpieczenie tych danych przed ich utratą, wyciekiem, czy niepożądanym dostępem - niedopuszczenie do sytuacji, aby te dane były przetwarzane przez osoby niemające do tego upoważnienia. Przepisy o ochronie danych osobowych nie wskazują konkretnych rodzajów zabezpieczeń, ponieważ co znajdzie zastosowanie w małym biurze rachunkowym, może już nie być skuteczne w dużej korporacji. Dobór odpowiednich zabezpieczeń zależy od konkretnej firmy.

ZAPAMIĘTAJ

W każdej jednostce organizacyjnej należy dokładnie określić obieg informacji zawierających dane osobowe i starannie wybrać pracowników, którzy będą mieli do nich dostęp. Działania administratora bezpieczeństwa informacji powinny zapewnić twierdzące odpowiedzi na poniższe pytania.

- Czy w internecie nie udostępnia się prywatnych danych pracowników bez ich zgody?
- Czy pracownicy nie wynoszą na zewnątrz danych osobowych klientów i czy są świadomi odpowiedzialności karnej za nielegalne udostępnianie danych osobowych?
- Czy każdy pracownik stosuje się do obowiązku niszczenia dokumentów zawierających dane osobowe w przeznaczonych do tego celu niszczeniach?
- Czy zużyte nośniki informacji są właściwie utylizowane?