



DR WOJCIECH RAFAŁ WIEWIÓROWSKI – GENERALNY  
INSPEKTOR OCHRONY DANYCH OSOBOWYCH – WYJAŚNIA



#### PYTANIE:

**Czy związek zawodowy ma prawo pozyskiwać od pracodawcy dane osobowe pracownika i przechowywać je w celu ewentualnego późniejszego wykorzystania?**

#### ODPOWIEDŹ:

**Nie, gdyż pozyskiwanie danych na zapas i ich przechowywanie w bliżej nieokreślonym celu z zamiarem ewentualnego późniejszego wykorzystania jest bezprawne i narusza przepisy ustawy o ochronie danych osobowych.**

#### UZASADNIENIE:

Przechowywanie danych osobowych stanowi jedną z form ich przetwarzania. Przez przetwarzanie danych należy rozumieć jakiegokolwiek operację wykonywaną na danych osobowych.

Ponadto ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (zwana dalej ustawą) stanowi, że aby przetwarzanie danych osobowych było legalne, musi zostać spełniona przynajmniej jedna z przesłanek określonych w art. 23 ust. 1 ustawy (w przypadku danych osobowych tzw. zwykłych, jak np. imię, nazwisko, adres zamieszkania) lub w art. 27 ust. 2 ustawy (jeśli wykorzystywane byłyby dane tzw. szczególnie chronione, do których zalicza się m.in. dane o przynależności związkowej).

Co ważne, przesłanka musi istnieć zarówno w momencie pozyskiwania danych osobowych, jak i w czasie ich przechowywania.

A zatem za niezgodne z prawem należy uznać np. nie tylko pozyskanie, ale i przechowywanie przez związek zawodowy bez wskazania podstawy prawnej danych osobowych pracowników takich jak: imię i nazwisko, data i miejsce urodzenia, adres stałego zameldowania, adres do korespondencji, numer PESEL, seria i numer dowodu osobistego, stanowisko, data zatrudnienia.

Artykuł 28 ustawy z 23 maja 1991 r. o związkach zawodowych stanowi, że pracodawca jest zobowiązany udzielić na żądanie związku zawodowego informacji niezbędnych do prowadzenia działalności związkowej, w szczególności informacji dotyczących warunków pracy i zasad wynagradzania, często jest wskazywany przez związek zawodowy jako podstawa do udostępniania mu danych osobowych. Przepis ten nie jest jednak uniwersalną podstawą do udostępniania związkowi danych osobowych pracowników bez ich zgody. Przy czym wymienione wyżej dane osobowe pracowników trudno uznać za informacje, o których mowa w art. 28 ustawy o związkach zawodowych.

Uzasadnieniem usprawiedliwiającym przekazanie danych nie może też być przypuszczenie, że dane te mogą być potrzebne w przyszłości. Przechowywanie danych osobowych z zamiarem ich ewentualnego, późniejszego wykorzystania w celu zrealizowania hipotetycznego, przyszłego obowiązku, który na związek zawodowy mogą nałożyć nowe przepisy prawa, nie znajduje podstawy prawnej w przepisach ustawy. Aby taki obowiązek nałożony przepisami prawa stanowił przesłankę uzasadniającą przetwarzanie danych osobowych, wskazaną w art. 23 ust. 1 pkt 2 ustawy (stanowiącym, że przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa), musi istnieć w momencie przetwarzania tych danych. Przechowywanie danych osobowych bez podstawy określonej w przepisach ustawy, czyli niejako „na zapas”, stanowi naruszenie obowiązku zapewnienia, aby dane te były przetwarzane zgodnie z prawem (art. 26 ust. 1 pkt 1 ustawy), a także, aby dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 4 ustawy).

Reasumując, związek zawodowy ma prawo pozyskiwać od pracodawcy dane osobowe pracowników tylko wówczas, gdy spełnia jeden z warunków legalizujących przetwarzanie danych osobowych. Jednak takich danych pozyskanych w określonym prawnie uzasadnionym celu nie ma prawa przechowywać, jeśli cel przechowywania jest bliżej niesprecyzowany, a jego realizacja odległa w czasie.

## PYTANIE: \_\_\_\_\_

Czy pracodawca odpowiada za to, że jego pracownik ujawnił informacje o osobie starającej się o pracę, które pozyskał z dokumentów rekrutacyjnych?

## ODPOWIEDŹ: \_\_\_\_\_

Tak, gdyż jako administrator danych ma obowiązek dbania o to, aby dane osobowe były odpowiednio zabezpieczone.

## UZASADNIENIE: \_\_\_\_\_

Jednym z podstawowych obowiązków administratora danych osobowych jest dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą (art. 26 ust. 1 pkt 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, dalej zwana ustawą). Ta generalna zasada znajduje swoje rozwinięcie w innych przepisach wskazanej ustawy określającej m.in. wymogi, jakie powinien spełniać administrator danych w celu zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Jednym z podstawowych obowiązków spoczywających na administratorze jest obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym (art. 36 ust. 1 ustawy).

W sytuacji gdy pracownik uzyskał dostęp do danych osobowych innych osób, np. w związku z postępowaniem rekrutacyjnym, ma on bezwzględny obowiązek zachowania poufności przetwarzanych danych. Natomiast udostępnienie tych danych osobom nieupoważnionym obciąża nie tylko pracownika, ale również administratora danych, który ponosi pełną odpowiedzialność za ich przetwarzanie. Niedopuszczalne jest zatem udostępnienie przez pracownika osobie nieupoważnionej danych osobowych pozyskanych podczas wykonywania przez niego obowiązków służbowych.

Z ustawy o ochronie danych osobowych wynika, że administrator danych musi mieć pełną kontrolę nad procesem przetwarzania danych, tak aby zapobiec powstawaniu zdarzeń narażających dane na udostępnienie osobom nieupoważnionym. Musi też mieć pełną wiedzę na temat całości procesu przetwarzania oraz weryfikować zachowanie pracowników pod kątem przestrzegania przez nich zasad ochrony danych osobowych. Administrator odpowiada bowiem za działania podejmowane przez pracowników, co potwierdza nie tylko doktryna, ale i utrwalone orzecznictwo administracyjne (por. wyrok Naczelnego Sądu Administracyjnego z 4 kwietnia 2003 r., II SA 2935/02, nie publ.).

Za nieprzestrzeganie wskazanych obowiązków ustawa o ochronie danych osobowych przewiduje odpowiedzialność karną. Jej przepisy przewidują karę grzywny, ograniczenia wolności albo pozbawienia wolności do 2 lat dla tego, kto – administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych – udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym (art. 51 ust. 1 ustawy). Karane jest także nieumyślne naruszenie obowiązku zabezpieczenia danych przed ich zabránem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem (art. 52 ustawy).