



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

**DOLiS-035-2097/14**

**Warszawa, dnia            grudnia 2014 r.**

**Prezes Zarządu**

**w związku z uzyskaniem przez Generalnego Inspektora Ochrony Danych Osobowych informacji o przekazywaniu danych osobowych pracowników przez przedstawicielstwo firmy [...], firmie [...], działając na podstawie art. 19a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182), zgodnie z którym Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych, zwracam się o podjęcie stosownych działań celem zapewnienia podstaw prawnych do powyższego przekazywania.**

Generalny Inspektor Ochrony Danych Osobowych pozyskał od Okręgowego Inspektoratu Pracy informację, że przedstawicielstwo firmy [...] przekazuje dane pracowników firmie [...] w związku ze szkoleniami BHP, bez wymaganej przepisami ustawy o ochronie danych ustawowych podstawy prawnej.

Mając na uwadze powyższe organ ochrony danych osobowych wskazuje, że podmioty przetwarzające dane osobowe są obowiązane do stosowania przepisów ustawy o ochronie danych osobowych na każdym etapie przetwarzania tych danych, zarówno w sytuacji, gdy zbierają dane, przechowują je, czy też udostępniają. W świetle przepisów ustawy o ochronie

danych osobowych do podstawowych obowiązków administratora danych należy spełnienie jednej z przesłanek legalności przetwarzania (w tym udostępniania) danych, które w odniesieniu do danych osobowych tzw. zwykłych określone zostały w art. 23 ust. 1 ustawy. Zastrzec należy, że dane szczególnie chronione, określone w art. 27 ust. 1 ustawy podlegają bardziej restrykcyjnej ochronie. Zgodnie z art. 27 wymienionej ustawy przetwarzanie powyższych danych jest co do zasady zabronione, a zasada ta doznaje wyjątków jedynie w przypadkach enumeratywnie wyliczonych w art. 27 ust. 2 ustawy.

Mocą art. 26 ust. 1 pkt 1-3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem (pkt 1), zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 (pkt 2), merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (pkt 3).

Wskazuję również, że w uzasadnionych przypadkach stosowną podstawą przekazania danych osobowych przez ich administratora innemu podmiotowi może być zawarta na piśmie pomiędzy tym podmiotem a administratorem danych umowa powierzenia przetwarzania danych, o której mowa w art. 31 wymienionej ustawy. Zgodnie z tym przepisem administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot ten może przetwarzać dane wyłącznie w celu i zakresie przewidzianym w umowie (art. 31 ust. 2). Umowa taka musi określać zakres i cel przetwarzania danych, które zostały powierzone. Podmiot, któremu przetwarzanie danych zostało powierzone na mocy art. 31 ustawy o ochronie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 – 39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy tj. przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Podkreślenia wymaga, iż w zakresie przestrzegania tych przepisów podmiot ten ponosi odpowiedzialność jak administrator danych (art. 31 ust. 3). Ponadto, jest on związany w swej działalności zakresem i celem przetwarzania w przedmiotowej umowie wyznaczonym. Może zatem przetwarzać dane wyłącznie w takim zakresie i celu, jaki został przewidziany w jej treści. Przedmiotem powierzenia przetwarzania danych osobowych może być przy tym zarówno kompleksowa

obsługa procesu przetwarzania danych dla określonego celu, jak i jedynie tylko niektóre operacje na danych, jak np. ich przechowywanie czy usuwanie. Powierzenie przetwarzania danych osobowych następuje bez konieczności uzyskiwania zgody osób, których dane dotyczą.

Należy również pamiętać, że administrator danych zawierając umowę powierzenia danych jest zobowiązany do stałej koordynacji procesu jej wykonywania. Powierzenie przetwarzania danych osobowych, o którym mowa w art. 31 ustawy, nie oznacza też zmiany statusu administratora danych osobowych, tj. pozostaje on podmiotem decydującym o celach o środkach przetwarzania danych osobowych, natomiast podmiot prowadzący działalność w imieniu i na rzecz administratora danych nie ma możliwości jakiegokolwiek wykorzystania tychże danych do własnych celów, czy potrzeb.

Podsumowując stwierdzić należy, że aby przekazywanie danych osobowych innemu podmiotowi było legalne, konieczne jest istnienie ku temu odpowiedniej podstawy prawnej, tj. spełnienie przesłanki z art. 23 ust. 1 lub art. 27 ust. 2 ustawy o ochronie danych osobowych ewentualnie zawarcie umowy powierzenie przetwarzania danych osobowych zgodnie z art. 31 ust. 1 tejże ustawy. Nadmienić wypada, że skorzystanie z ostatniego z wymienionych przepisów jest rozwiązaniem najczęściej spotykanym w przypadkach zlecenia wykonywania określonych zadań pracodawcy podmiotom zewnętrznym, np. przeprowadzania szkoleń BHP. Powtórzyć także trzeba, że powierzenie przetwarzania danych nie oznacza wyzbycia się statusu podmiotu decydującego o celach i środkach przetwarzania, nie oznacza innymi słowy zmiany administratora danych czy możliwości przetwarzania danych przez podmiot, któremu powierzono dla jego własnych celów.

W kontekście przedmiotowej sprawy należy ponadto zwrócić uwagę na obowiązek właściwego zabezpieczenia danych. Obowiązek ten wynika w szczególności z rozdziału 5 powołanej ustawy, jak i rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Na administratorze danych spoczywa wynikający z art. 36 ust. 1 ustawy obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Innymi słowy art. 36 ust. 1 ustawy zobowiązuje każdego administratora danych do wprowadzenia takich środków oraz rozwiązań technicznych i organizacyjnych, które zapewnią danym osobowym, w konkretnych warunkach i okolicznościach przetwarzania,

skuteczną ochronę przed potencjalnymi zagrożeniami. Jak już wyżej wspomniano, również podmiot, któremu przetwarzanie danych zostało powierzone na mocy art. 31 ustawy o ochronie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć odpowiednie środki zabezpieczające zbiór danych. Jednocześnie cały proces przetwarzania danych w imieniu i na rzecz ich administratora powinien być bezpieczny, tj. odpowiadać wspomnianym zasadom bezpieczeństwa.

Niewywiązanie się z obowiązku właściwego zabezpieczenia danych może w konsekwencji prowadzić do powstania odpowiedzialności karnej. Przepisy karne ustawy o ochronie danych osobowych dotyczące niedopełnienia obowiązków w zakresie właściwego zabezpieczenia danych osobowych poprzez użycie określeń „administrujący zbiorem”, „administrujący danymi osobowymi”, „obowiązany do ochrony danych osobowych” wskazują, kto może odpowiadać za właściwe zabezpieczenie danych osobowych. Sprawcą czynu z art. 51 lub 52 ustawy o ochronie danych osobowych może być, oprócz kierownika jednostki, również administrator bezpieczeństwa informacji lub każdy inny pracownik danej jednostki odpowiedzialny za ochronę danych, jak również każda osoba przetwarzająca dane osobowe na podstawie upoważnienia administratora danych.

W określonych przypadkach można również rozważać odpowiedzialność dyscyplinarną lub porządkową z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. 1998 r. Nr 21 poz. 94, ze zm.), czy innych przepisów szczególnych wobec ustawy o ochronie danych osobowych.

Mając na uwadze powyższe, proszę o odniesienie się do wskazanych kwestii, poprzez poinformowanie Generalnego Inspektora Ochrony Danych Osobowych o tym, jakie działania podjęto w celu usunięcia zasygnalizowanych nieprawidłowości.

Zaznaczam również, że zgodnie z art. 19a ust. 3 ustawy o ochronie danych osobowych, podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie **w terminie 30 dni od daty jego otrzymania.**