

## Kiedy udostępnić dane pracownika osobie z zewnątrz

Z informacjami osobowymi dotyczącymi pracowników mogą się zapoznać przedstawiciele różnych urzędów i instytucji. Uprawnienia te wynikają z wielu przepisów, odrębnych dla danego sektora działalności



dr WOJCIECH  
RAFAŁ  
WIEWIÓ-  
ROWSKI

generalny inspektor  
ochrony danych  
osobowych

Pracodawca musi pamiętać, że każdy, kto sięga (czy chce sięgnąć) po dane osobowe pracowników danego zakładu pracy, powinien wskazać podstawę prawną, która na dostęp do nich mu zezwala.

Podstawa musi mieć rangę ustawy, bowiem tylko z aktu prawnego tej rangi może wynikać uprawnienie danego podmiotu do zapoznania się z określonym rodzajem informacji. Dotyczy to wszystkich informacji, którymi dysponuje pracodawca, zarówno tzw. zwykłych, jak np. imię i nazwisko czy adres zamieszkania, jak i szczególnie chronionych, do których należą m.in. dane o stanie zdrowia czy przynależności związkowej.

### Instytucje uprawnione

Lista podmiotów, które mają takie uprawnienia, jest obszerna. Jednym z nich jest

Państwowa Inspekcja Pracy, która prowadząc postępowanie kontrolne, ma prawo żądać przedłożenia akt osobowych i wszelkich dokumentów związanych z wykonywaniem pracy przez pracowników. Z kolei ustawa o komornikach sądowych i egzekucji zobowiązuje różnego rodzaju organy, urzędy i podmioty do udzielenia komornikowi na jego żądanie informacji niezbędnych do prawidłowego prowadzenia postępowania egzekucyjnego.

O dostęp do danych osobowych mogą też występować: Policja, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu czy Służba Celna, a uprawnienie to wynika z przepisów, na podstawie których te służby działają. Podobnie jest w przypadku inspektorów GIO-DO przeprowadzających kontrole, których ustawa o ochronie danych osobowych (dalej ustawa) uprawnia m.in. do wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli.

Pracodawca, przed udostępnieniem danych osobowych, powinien więc sprawdzić, czy ten, kto chce je uzyskać, jest do tego uprawniony na mocy

przepisów prawa, a niekiedy również to, czy posiada odpowiednie upoważnienie wydane przez instytucję, którą reprezentuje.

### Ewidencja i wgląd do akt

Nie ma ogólnej reguły co do tego, czy pracodawca powinien być w odpowiednim czasie uprzedzony, że jakiś podmiot chce sięgnąć do danych osobowych jego pracowników. To zależy od tego, co ma być powodem wglądu do takich informacji. Istotne jest także, jaki podmiot o dostęp do nich się ubiega. Jeśli celem jest kontrola, z reguły powiadamia się o niej nie później niż na siedem dni przed jej rozpoczęciem. Oczywiście, w szczególnych sytuacjach organy ścigania czy inspekcje mogą sięgnąć po dane w każdej chwili, bez uprzedzenia. Pracownicy biura GIO-DO informują o planowanej kontroli z co najmniej siedmiodniowym wyprzedzeniem.

Pracodawca, jak każdy administrator danych osobowych, ma obowiązek zapewnić właściwą ochronę danych osobowych oraz kontrolę nad tym, jakie dane osobowe, kiedy, przez kogo i komu są przekazywane. Temu celowi słu-

ży m.in. odnotowywanie, kto, kiedy i do jakich danych uzyskuje dostęp. Nie w każdym przypadku jest to jednak wymagane - zależy od tego, czy dany podmiot jest odbiorcą danych w rozumieniu ustawy o ochronie danych osobowych. Przez odbiorcę danych rozumie się każdego, komu dane są udostępnione, z wyłączeniem np. osoby, której one dotyczą, osoby upoważnionej do przetwarzania danych czy organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Trzeba przy tym dodać, że osoby, które upoważniono do przetwarzania danych, są zobowiązane zachować w tajemnicy nie tylko pozyskane informacje, ale również sposoby ich zabezpieczenia. Zgodnie z przepisami ustawy, za niedotrzymanie tajemnicy grozi odpowiedzialność karna w postaci kary grzywny, kary ograniczenia wolności albo pozbawienia wolności do lat dwóch.

### Informacje dla kontrahenta

Kontrahent pracodawcy nie ma prawa sięgania po dane

jego podwładnych tylko dlatego, że jest jego partnerem gospodarczym. Można jednak wyobrazić sobie sytuacje szczególne, w których takie uprawnienie może posiadać, mając do tego odpowiednią podstawę prawną.

Kontrahentem może być np. służba specjalna, dla której znaczenie mogą mieć np. informacje dotyczące szczególnych uprawnień pracowników, którzy będą osobiście wykonywali pracę zleconą na rzecz tej służby. Takie sytuacje są jednak wyjątkowe. Niedopuszczalne jest natomiast, aby za podstawę prawną do udostępnienia kontrahentowi pracodawcy informacji z prowadzonych przez niego akt personalnych uznano zgodę pracownika. Zgoda jest zawsze wątpliwą podstawą prawną do przetwarzania danych osobowych w relacjach pracodawca - pracownik. Istniejący w nich brak równowagi stron stawia bowiem pod znakiem zapytania dobrowolność wyrażania przez pracownika zgody na przetwarzanie jego danych osobowych.

Niekiedy jednak umożliwienie dostępu do danych osobowych zgromadzonych przez pracodawcę bywa konieczne.

Tak jest m.in. wówczas, gdy pracodawca zleca podmiotom zewnętrznym wykonanie określonych usług, np. naprawę oprogramowania, za pomocą którego przetwarzane są dane osobowe pracowników lub klientów. Serwisanci, aby ustalić przyczynę awarii i usunąć usterkę, muszą uzyskać dostęp do baz danych pracodawcy. Dlatego umowa zawierana z firmą serwisującą sprzęt czy oprogramowanie powinna określać sposoby zabezpieczenia danych osobowych, do których serwisanci będą mieli dostęp, tak aby zagwarantować, że nikt inny poza nimi nie będzie miał do nich dostępu.

Natomiast gdyby naprawę systemu informatycznego dokonywały osoby zatrudniane przez pracodawcę, a przy usuwaniu usterki użytkowałyby dostęp do bazy danych osobowych, np. danych wszystkich zatrudnionych, to powinny posiadać nadane przez pracodawcę upoważnienie do przetwarzania danych osobowych.

### Podstawa prawna

Art. 31 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.).